VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS

STATISTICKÝ VÝSTUP Z ASISTOVANÝCH ZHODNOCENÍ
STATISTICAL OUTPUT OF SECURITY AUDITS

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — **Ing. Gabriela Hrubešová**
AUTHOR

VEDOUCÍ PRÁCE — **Ing. Petr Sedlák**
SUPERVISOR

BRNO 2019

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání diplomové práce

Ústav:	Ústav informatiky
Studentka:	**Ing. Gabriela Hrubešová**
Studijní program:	Systémové inženýrství a informatika
Studijní obor:	Informační management
Vedoucí práce:	**Ing. Petr Sedlák**
Akademický rok:	2018/19

Ředitel ústavu Vám v souladu se zákonem č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů a se Studijním a zkušebním řádem VUT v Brně zadává diplomovou práci s názvem:

Statistický výstup z asistovaných zhodnocení

Charakteristika problematiky úkolu:

Úvod
Cíle práce, metody a postupy zpracování
Teoretická východiska práce
Analýza současného stavu
Návrh řešení a přínos návrhů řešení
Závěr
Seznam použité literatury
Přílohy

Cíle, kterých má být dosaženo:

Cílem této diplomové práce je statistická analýza asistovaných zhodnocení.

Základní literární prameny:

ČSN ISO/IEC 27001. Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnostiinformací - Požadavky, Praha: Český normalizační institut, 2014.

ČSN ISO/IEC 27002. Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnostiinformací - Soubor postupů, Praha: Český normalizační institut, 2014.

DOUCEK Petr, Luděk NOVÁK a Vlasta SVATÁ. Řízení bezpečnosti informací. Praha: Professional Publishing, 2008. ISBN 80-86898-38-5.

ONDRÁK Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. Problematika ISMS v manažerské informatice. Brno: CERM, Akademické nakladatelství, 2013. ISBN 978-80-7204-872-4.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2018/19

V Brně dne 28.2.2019

L. S.

doc. RNDr. Bedřich Půža, CSc. ředitel	doc. Ing. et Ing. Stanislav Škapa, Ph.D. děkan

Abstrakt

Předmětem této diplomové práce je statistická analýza asistovaných zhodnocení. Teoretická část popisuje klíčové pojmy z oblasti kybernetické a informační bezpečnosti, základní podklady pro tuto oblast a důležité předpisy. Další část se zaměřuje na popis asistovaného zhodnocení, jeho průběhu, nutných podmínek a obsahu. V poslední části se věnujeme statistické analýze získaných vzorků. Vzorky analyzujeme z několika úhlů pohledu, porovnáváme a hledáme vlastnosti a informace, které by mohly být nápomocné pro auditory při hodnocení.

Abstract

The subject of this diploma thesis is a statistical analysis of security audits. The theoretical part describes key terms in the field of cyber and information security, basic background for this area and important regulations. The next part focuses on the description of security audit, its course, necessary conditions and content. The last part is devoted to statistical analysis of obtained samples. We analyse samples from several points of view, compare and look for features and information that could be helpful to the auditor's assessment.

klíčová slova

asistované zhodnocení, KII, VIS, GDPR, informační bezpečnost, kybernetická bezpečnost, analýza

key words

security audit, CII, IIS, GDPR, information security, cyber security, analysis

HRUBEŠOVÁ, Gabriela. *Statistický výstup z asistovaných zhodnocení* [online]. Brno, 2019 [cit. 2019-05-05]. Dostupné z: https://www.vutbr.cz/studenti/zav-prace/detail/119720. Diplomová práce. Vysoké učení technické v Brně, Fakulta podnikatelská, Ústav informatiky. Vedoucí práce Petr Sedlák.

Čestné prohlášení

Prohlašuji, že předložená diplomová práce je původní a zpracovala jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem ve své práci neporušila autorská práva (ve smyslu Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně dne 6. května 2019

.....

podpis studenta

Děkuji svému školiteli Ing. Sedlákovi za četné rady a připomínky při vedení mé diplomové práce. Také chci poděkovat panu Ing. Svobodovi za odbornou oponenturu.

Ing. Gabriela Hrubešová

Obsah

ÚVOD

Vývoj nových informačních a komunikačních technologií se neustále zrychluje a jejich přítomnost dnes nalezneme ve všech oblastech. Svět je v dnešní době závislý na těchto technologiích. Rozvoj informatiky však nese i negativní následky. Hledí se totiž na rychlost a novost technologií a opomíjí se jejich bezpečnostní stránka. Kritériem pro výběr technologie však není bezpečnost, ale výkon a to, jaké snížení nákladů může tato technologie přinést. Technologie mohou být zneužity a může díky nim vznikat velké množství hrozeb. To může přinést mnohem větší a z pohledu nákladů vyšší ztrátu, než jaký přínost společnosti technologie přinese.

Organizace, které využívají informační a komunikační technologie by měly být připraveny čelit možným hrozbám, které plynou z užívání těchto technologií. Měly by tyto hrozby identifikovat, analyzovat je a nalézt opatření, které mohou působení hrozeb eliminovat nebo alespoň zmírnit. Zajištění dostatečné úrovně bezpečnosti vychází ze zkušeností a ze znalosti aktuálního stavu. Pokud neznáme reálnou situaci, nemůžeme identifikovat slabá místa a sjednat nápravy či vylepšení. Proto je velmi důležité provádět asistované zhodnocení, díky kterému odhalíme rizika, hrozby a části bezpečnosti, které negativně působí na informační bezpečnost a ovlivňují dostupnost, důvěrnost a integritu.

Asistovaná zhodnocení jsou zcela novým způsobem, jak zjistit aktuální stav kybernetické a informační bezpečnosti konkrétní společnosti nebo systému. Pro analytiky, ale také společnosti, které budou hodnoceny, je vhodné znát vlastnosti asistovaného zhodnocení. Prozatím neexistuje mnoho informací o tomto způsobu zjištění bezpečnostní situace společnosti nebo jen systému, a proto bude tato práce sloužit jako náhled do tohoto tématu.

Cílem je zanalyzovat několik vybraných vzorků asistovaného zhodnocení, které byly získány provedením bezpečnostního auditu u vybraných firem. Vzorky popisují tedy reálnou praxi. Zadáním práce bylo získat velké množství informací z dat, která nám byla poskytnuta. Osoba, která bude vypracovávat asistované zhodnocení by měla mít povědomí o stavech, ve kterých se nachází jiné společnosti, měla by mít možnosti pro srovnání, možnost uvedení příkladu apod. Tyto poznatky by měla tato diplomová práce nabídnout.

Práce nám také osvětlí situaci kybernetické a informační bezpečnosti na území ČR. Jelikož jde o analýzu vzorků, které podnikají nebo provádějí svou činnost zde, získáme náhled na to, jak se tyto společnosti vypořádají s hrozbami a opatřeními na reálném poli.

1 VYMEZENÍ PROBLÉMU A CÍLE PRÁCE

Cílem této práce je statistická analýza asistovaných zhodnocení. Chceme zkoumat získané vzorky asistovaných zhodnocení a nalézt informace či vlastnosti, které nejsou na první pohled z dat jasně vidět. Zjištěné poznatky poslouží auditorům jako doplňující podklad pro společnosti, které odpovídají vzorkům v této práci. Dále poslouží k práci auditorů či analytiků na dalších asistovaných zhodnoceních. Dále bude práce sloužit jako sbírka vzorků k porovnání s dalšími asistovanými zhodnoceními. Jedná se také o jakýsi indikátor aktuálního stavu kybernetické a informační bezpečnosti v ČR. Část, ve které půjde o analýzu konkrétního vzorku, může sloužit jako jakási metodika nebo příručka k postupu a formě dodatečného analyzování jiného vzorku.

Ústředním tématem této práce jsou asistovaná zhodnocení a jejich analýza. Získáním 34 vzorků jsme vytvořili soubor dat, která mohou být analyzována. Asistovaná zhodnocení jsou postavena na zákoně o kybernetické bezpečnosti a jeho prováděcích vyhláškách, na vyhlášce o kybernetické bezpečnosti, směrnicích a normách z oblasti bezpečnosti a na nařízení Rady EU. Proto jsou v teoretické části popsány všechny normalizační instituce a normy, zákony, vyhlášky a nařízení z oblasti informační a kybernetické bezpečnosti. Jsou zde uvedeny zákony a normy využívané převážně v asistovaném zhodnocení.

Dále jsou v práci popsány nejdůležitější pojmy, jejichž pochopení je potřebné ke studiu dalšího textu práce. V další části práce bude popsáno asistované zhodnocení. Uvedeme způsob získání dat, jejich popis a způsob práce s nimi. Také zde nalezneme podmínky pro provedení asistovaného zhodnocení nebo důvody k jeho vypracování. Tato část vysvětluje formu asistovaného zhodnocení, části a oblasti, které se v něm vyskytují. Na závěr této kapitoly jsou popsány výsledky, které jsou získány z asistovaného zhodnocení, tedy jaký je výstup a způsob hodnocení.

Návrhová část řeší již analýzu získaných vzorků asistovaných zhodnocení. Pokusíme se nalézt vlastnosti, které by mohly být využity v praxi při provádění dalších asistovaných zhodnocení. Provedeme analýzu všech vzorků společně, poté vzorky rozdělíme do různých skupin dle velikosti, oboru podnikání nebo toho, zda se jedná o prvky kritické informační infrastruktury nebo správce významného informačního systému. Následně je

zvolen jeden vzorek, který bude zkoumán detailněji. Na závěr této kapitoly se zamyslíme nad spojením asistovaného zhodnocení a systémové integrace.

Toto téma jsem si vybrala pro jeho významnost a aktuálnost a také proto, že ráda zjišťuji na první pohled neviditelné poznatky z velkého množství dat. Motivací je nalézt informace a vlastnosti ze získaných vzorků, které mohou pomoci při dalším vypracování asistovaných zhodnocení, ale také při hodnocení, porovnávání a analýze společností, u kterých bude vypracováno asistované zhodnocení.

2 TEORETICKÁ VÝCHODISKA PRÁCE

V této kapitole budou uvedeny teoretické poznatky potřebné k pochopení problematiky této diplomové práce. V první části jsou základní pojmy z oblasti bezpečnosti v IT. Dále se zaměříme na normalizační instituce, normy a legislativu, které jsou často využívané při provádění asistovaných zhodnocení a jiných bezpečnostních auditů. Poté budou uvedeny informace o systému řízení bezpečnosti informací, popíšeme si zjednodušeně postup zavádění ISMS. Vysvětlíme si pojmy kritická informační infrastruktura a významný informační systém.

2.1 Základní pojmy

Tato podkapitola obsahuje základní pojmy z oblasti bezpečnosti v IT. Zjistíme, co je informační bezpečnost, co je to bezpečnost organizace a IS/ICT a co je to kybernetické bezpečnost. Popíšeme triádu CIA využívanou v bezpečnosti.

Informační bezpečnost

Informační bezpečnost neboli bezpečnost informací je brána jako ochrana před poškozením, zničením, ztrátou nebo zcizením dat, a to z pohledu triády CIA (confidentiality, integrity, availability). Informační bezpečnost se týká organizace. Můžeme ji dále dělit na fyzickou, personální, organizační a komunikační [1].

Informační bezpečnosti se dosahuje pomocí zavádění vhodných sad bezpečnostních opatření. Tato opatření jsou získána procesem řízení rizik a poté jsou spravovány pomocí systému řízení bezpečnosti informací [2].

Bezpečnost organizace a IS/ICT

Informační bezpečnost je ve vzájemném vztahu s bezpečností organizace a bezpečností IS/ICT. Bezpečnost organizace zabezpečuje objekt a majetek organizace. Aktiva informačních systémů, které jsou podporovány informačními a komunikačními technologiemi řeší bezpečnost IS/ICT [3].

Kybernetická bezpečnost

Kybernetická bezpečnost se týká kybernetického prostoru. Kybernetická bezpečnost je souhrnem technických, organizačních, vzdělávacích a právních prostředků, které obstarávají ochranu kybernetického prostoru [1].

Kybernetická bezpečnost se omylně zaměňuje nebo dokonce dává do rovnosti. Kybernetická a informační bezpečnost se někdy překrývají, rozdílem je však perimetr. Jak už bylo zmíněno kybernetická bezpečnost se týká kybernetického prostoru a informační bezpečnost se týká organizace. Dokážeme nalézt příklad hrozby, které jsou zahrnuty v informační bezpečnosti, ale ne v kybernetické bezpečnosti. Například tedy odcizení šanonu s dokumenty z kanceláře zaměstnance [4].

Rozdíl těchto dvou bezpečností potvrzuje i orgán pro kybernetickou bezpečnost v ČR, Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB). V České republice je kybernetická bezpečnost zahrnuta v zákonech a vyhláškách. Ty vyšly v roce 2014 a dále pak vyšly novely, které je upravují.

Triáda CIA

Cílem bezpečnosti informací je dosažení takzvané triády CIA:

- **C - confidentiality (důvěrnost)** - znamená poskytovat informace pouze procesům, entitám a uživatelům, kteří jsou k tomu oprávněni [3].
- **I - integrity (integrita)** - je zajištění úplnosti a správnosti informací [3].
- **A - availability (dostupnost)** - znamená, že informace bude oprávněnému uživateli přístupná v okamžiku, kdy o ni žádá [3].

2.2 Normalizační instituce

Tato podkapitola specifikuje normalizační instituce, které tvoří normy využívané v bezpečnosti v oboru ICT.

ISO – International Organization for Standardization

Tato organizace je nezávislá a nadnárodní. Podporuje rozvoj standardizační činností a působí celosvětově. Zaměřuje se na spolupráci na úrovni technologických, ekonomických, vědeckých a intelektuálních aktivit a také na usnadnění mezinárodních směn služeb a zboží [3].

IEC – International Electrotechnical Comission

Jde o organizací, která působí na celém světě. Připravuje a publikuje normy pro veškeré elektronické, elektrotechnické a jiné technologie vztahující se k nim. Společně s ISO a ITU patří mezi tři největší globální instituce [3].

ITU - International Telecommunications Union

ITU je opět celosvětová normalizační instituce. Mobilní technologie, internet nebo mnoho dalších technologií tato instituce podpořila. Je vedoucí institucí ve správě spekter rádiové frekvence. Společně s ISO a IEC tvoří trojici největších globálních institucí [3].

NIST – National Institute for Standards and Technology

Tato instituce je americká normalizační organizace. Pracuje v oblasti vývoje a podpory standardů, technologií a měřících technik. Jejím účelem je zlepšení života, dále pak zvýšení produktivity a usnadnění obchodu [3].

ČAS – Česká agentura pro standardizaci

Tuto agenturu zřídil Úřad pro technologickou normalizaci, metrologii a státní zkušebnictví (ÚNMZ). Jde o státní příspěvkovou organizaci, která zodpovídá za veškeré činnosti v rámci tvorby, vydávání a distribuce technických norem [5].

ČSN - Česká technická norma, dříve Česká státní norma

Jde o přejímané evropské a mezinárodní normy, popřípadě o původní normy vyplývající z národních potřeb [3].

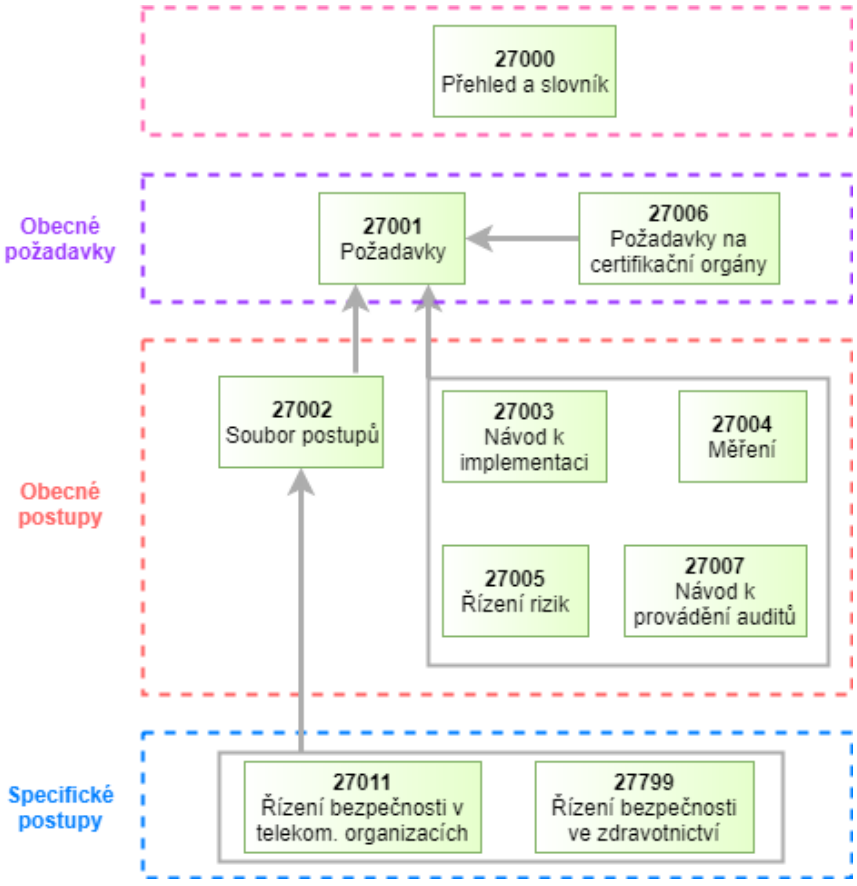
2.3 Normy vztahující se k informační a kybernetické bezpečnosti

Nejvyužívanější normy při provádění asistovaných zhodnocení a jiných bezpečnostních auditů budou uvedeny v této podkapitole. Norma je pouze doporučením pro dané řešení nebo standard. Standard je dokument popisující přesně stanovená kritéria a technické specifikace, které jsou používána jako pravidla, směrnice [3].

ISO/IEC 27K

Řada norem ISO/IEC 27000 se také nazývá řadou norem ISMS. Jde o mezinárodní normy pro systémy řízení, pro jejich zřízení a provoz. Pokud organizace budou postupovat dle norem, jsou schopny zavést a provozovat ISMS [2].

Do této řady spadají čtyři typy norem, normy popisující směrnice specifické pro odvětví, normy popisující obecné směrnice, normy specifikující požadavky a norma obsahující terminologii [2].



Obrázek 1: ISO/IEC normy řady 27000.[Zdroj: vlastní zpracování]

Veškeré normy v této řade jsou původně v anglickém jazyce a do ČSN nejsou přejaty všechny.

2.3.1 Normy obsahující terminologii

Mezi normy obsahující terminologii patří ISO/IEC 27000, její obsah popíšeme v této části.

ISO/IEC 27000 - Systémy řízení bezpečnosti informací – Přehled a slovník

První normou je ISO/IEC 27000, která je slovníkem a přehledem terminologie v normách řady ISO/IEC 27K. Jde o jakýsi úvod k ISMS. Tato norma poskytuje i přehled všech norem v řadě ISMS [2].

V roce 2018 byla tato norma zrevidována a bylo změněno několik věcí. Byl přepsán úvod celé normy, dále byly odebrány některé pojmy a definice, došlo k aktualizaci některých kapitol a odebrání některých příloh [2].

2.3.2 Normy specifikující požadavky

Normy, které specifikují požadavky na systém řízení bezpečnosti informací, dále požadavky na orgány provádějící audit a certifikaci těchto systémů a požadavky pro použití ve specifických odvětvích si přiblížíme v této části. Jde především o tyto normy: ISO/IEC 27001, ISO/IEC 27006, ISO/IEC 27009.

ISO/IEC 27001 - Systémy řízení bezpečnosti informací – Požadavky

Tato norma definuje požadavky na zavedení, implementaci, provoz, monitoring, přezkoumání a zlepšování ISMS, a to v souladu s podnikovými riziky. cyklus formalizovaných ISMS v kontextu celkových rizik činností organizace. Jsou zde vymezeny požadavky na bezpečnostní opatření, která jsou přizpůsobena potřebám organizací nebo jejich částem [2].

ISO/IEC 27006 - Požadavky na orgány poskytující audit a certifikaci systémů řízení bezpečnosti informací

Tento dokument specifikuje oblast certifikací ISMS. Jsou zde definovány požadavky a návod pro orgány poskytující audit a certifikaci ISMS na základě normy ISO/IEC 27001 [2].

ISO/IEC 27009 - Používání ISO/IEC 27001 pro specifická odvětví – Požadavky

Definuje požadavky pro použití normy ISO/IEC 27001 ve specifických odvětvích (obor, oblast aplikace nebo trh). Tyto požadavky jsou však v souladu s požadavky normy ISO/IEC 27001 [2].

2.3.3 Normy popisující obecné směrnice

Tato část se věnuje normám, které popisují obecné směrnice. Patří sem normy ISO/IEC 27002, ISO/IEC 27003, ISO/IEC 27004, ISO/IEC 27005, ISO/IEC 27007, ISO/IEC TR 27008, ISO/IEC 27013, ISO/IEC 27014, ISO/IEC TR 27016.

ISO/IEC 27002 - Soubor postupů pro opatření bezpečnosti informací

Tato norma přináší obecně uznávané cíle opatření a opatření osvědčených postupů, pro použití při výběru a implementaci opatření, a to z důvodu dosažení informační bezpečnosti [2].

ISO/IEC 27003 - Směrnice pro implementaci systému řízení bezpečnosti informací

Dokument dává vysvětlení a návod k normě ISO/IEC 27001, tedy k zavedení ISMS v souladu s normou ISO/IEC 27001 [2].

ISO/IEC 27004 - Řízení bezpečnosti informací – Monitoring, měření, analýzy a vyhodnocení

Dokument poskytuje rámec pro měření, díky kterému jsme schopni posoudit efektivnost ISMS dle normy ISO/IEC 27001 [2].

ISO/IEC 27005 - Řízení rizik bezpečnosti informací

V této normě nalezneme směrnice pro řízení rizik bezpečnosti informací. Jde o směrnice vhodně pro naplnění všech požadavků řízení rizik bezpečnosti. Opět jsou v souladu s normou ISO/IEC 27001 [2].

ISO/IEC 27007 - Směrnice pro audit systémů řízení bezpečnosti informací

Tento dokument přináší směrnici k provádění auditů ISMS na základě iso normy ISO/IEC 27001 [2].

ISO/IEC TR 27008 - Směrnice pro audit opatření ISMS

Zde se jedná o směrnice k přezkoumání, implementaci a provozování opatření. Je zde uvedená také technická kontrola shody opatření IS dle norem stanovených konkrétní organizací. Tato norma se nazývá technickou zprávou, TR – Technical Report [2].

ISO/IEC 27013 - Návod pro integrovanou implementaci ISO/IEC 27001 a ISO/IEC 20000-1

Tato norma cílí na integrovanou implementaci ISMS specifikovaného v ISO/IEC 27001 a SMS (Systém řízení bezpečnosti) specifikovaného v ISO/IEC 20000-1. Slouží k lepšímu pochopení obou norem [2].

ISO/IEC 27014 - Správa bezpečnosti informací

Dává nám návod ke správě bezpečnosti informací. Díky němu mohou organizace hodnotit, řídit a monitorovat řízení bezpečnosti informací [2].

ISO/IEC TR 27016 - Řízení bezpečnosti informací – Organizační ekonomika

Jde opět o technickou zprávu, která doplňuje řadu norem ISO/IEC 27K o metody řešící ekonomickou stránku při ochraně aktiv organizace. Dále poskytuje příklady a modely pro aplikaci organizační ekonomiky bezpečnosti informací [2].

2.3.4 Normy popisující směrnice specifické pro odvětví

Poslední skupinou jsou normy, které popisují směrnice specifické pro různá odvětví. Zde patří normy ISO/IEC 27010, ISO/IEC 27011, ISO/IEC 27017, ISO/IEC 27018, ISO/IEC 27019 a ISO/IEC 27799.

ISO/IEC 27010 - Směrnice pro řízení bezpečnosti informací pro meziodvětvové komunikace a komunikace mezi organizacemi

Tento dokument je použitelný pro všechny formy sdílení a výměny citlivých informací, a to jak v komunikaci mezi organizační, tak vnitro organizační [2].

ISO/IEC 27011 - Směrnice pro řízení bezpečnosti informací pro telekomunikační organizace na základě ISO/IEC 27002

Zde najdeme směrnice pro implementaci opatření informační bezpečnosti v telekomunikačních organizacích [2].

ISO/IEC 27017 - Směrnice pro řízení bezpečnosti informací pro cloudové služby na základě ISO/IEC 27002

Tento dokument obsahuje směrnice pro opatření informační bezpečnosti použitelné pro poskytovatele cloudových služeb [2].

ISO/IEC 27018 – Směrnice o ochraně osobních údajů ve veřejných cloudech, které působí jako zpracovatelé osobních údajů

Směrnice poskytuje návody, opatření pro implementaci ochrany osobních údajů v souladu s ISO/IEC 29100 pro oblast cloud computingu [2].

ISO/IEC 27019 - Směrnice pro opatření bezpečnosti informací pro energetický průmysl

Poskytuje návod, speciální požadavky a opatření pro systémy používané energetickými společnosti [2].

ISO/IEC 27799 - Řízení bezpečnosti informací ve zdravotnictví využívající ISO/IEC 27002

Návod pro implementaci opatření popsaných v ISO/IEC 27002 tak, aby mohly být využívány pro řízení informační bezpečnosti ve zdravotnictví [2].

2.3.5 Normy NIST

NIST publikuje velké množství norem v různých oblastech. U nás se hojně užívají normy publikované v oblasti kybernetické a informační bezpečnosti. Dále si uvedeme ty nejdůležitější.

NISTIR 7298 Glossary of Key Information Security Terms – Slovník klíčových pojmů informační bezpečnosti

V tomto dokumentu nalezneme důležité pojmy informační bezpečnosti, které jsou využívány v dalších publikovaných normách NIST [6].

NIST SP 800-12 An Introduction to Information Security - Úvod do informační bezpečnosti

Tento dokument obsahuje přehled principů, bezpečnostní opatření a koncepty informační bezpečnosti, které mohou organizace využít k efektivnímu zabezpečení systémů a informací. Veškeré informace jsou prověřeny na federálních informačních systémech a organizacích [7].

NIST SP 800-53 Security and Privacy Controls for Federal Information Systems and Organizations - Bezpečnostní opatření pro federální informační systémy a organizace

Jde o katalog bezpečnostních opatření a návod k výběru bezpečnostních opatření k ochraně provozu, zaměstnanců, aktiv, ale také jiných organizací a státu před hrozbami kybernetického útoku, přírodních katastrof, lidských chyb atd. [8].

2.4 Legislativa

Tato podkapitola se věnuje legislativě v oblasti kybernetické bezpečnosti. Tato legislativa je využívána při provádění asistovaných zhodnocení a dalších bezpečnostních auditů. Nejdůležitější je zákon o kybernetické bezpečnosti a vyhláška o kybernetické bezpečnosti.

Zákon č. 181/2014 Sb. Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti, dále jen ZKB, vstoupil v platnost v roce 2014 a je účinný od roku 2015. V roce 2017 byl dvakrát novelizován. Tento zákon řeší práva a povinnosti osob, pravomoc a působnost orgánů veřejné moci v oblasti kybernetické bezpečnosti. Do tohoto zákona jsou zapracovány předpisy Evropské unie, jde o transpozici směrnice NIS. Zákon také upravuje zajištění bezpečnosti sítí elektronických komunikací a informačních systémů. Aktuální znění je z roku 2018 [9].

Zákon by měl určit základní úroveň bezpečnostních opatření, vylepšit detekování kybernetických bezpečnostních incidentů, zavést hlášení kybernetických bezpečnostních incidentů a systém opatření pro reakce na kybernetické bezpečnostní incidenty a také řešit činnost dohledových pracovišť [9].

Novelami vzniklo mnoho zásadních změn. Došlo k úpravě pokut a přestupků a rozšířila se pravomoc národního a vládního CERT. Zásadní a velmi důležitou změnou je vytvoření nových subjektů pro Provozovatele základních služeb a Poskytovatele digitálních služeb. Jsou zde specifikovány online tržiště, cloud a internetové vyhledávače [9].

V příloze (Příloha 1.) je uvedeno přehledové blokové schéma k zákonu a jeho prováděcím předpisům, které bylo zpracováno Národním úřadem pro kybernetickou a informační bezpečnost [10].

Další příloha (Příloha 2.) obsahuje schéma povinností orgánů a osob podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů [11].

Vyhláška č. 82/2018 Sb. Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)

Tato vyhláška o kybernetické bezpečnosti, dále jen VKB, je z roku 2018. Vyhláška zpracovává Směrnici NIS. Upravuje obsah a strukturu bezpečnostní dokumentace, dále obsah a rozsah bezpečnostních opatření, řeší typy, kategorie a hodnocení důležitosti kybernetických incidentů, hlášení kybernetického bezpečnostního incidentu, upravuje náležitosti oznámení o provedení reaktivního opatření a jeho výsledku, uvádí vzor oznámení kontaktních údajů a jeho formu a také způsob likvidace dat, provozních údajů, informací a jejich kopií [12].

Původní vyhláška byla uvedena v roce 2014, tu však nahradila výše uvedená vyhláška v roce 2018. Opatření a povinnosti, které jsou obsahem asistovaného zhodnocení vycházejí z velké části z této vyhlášky.

Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (Směrnice NIS)

Tato směrnice, dále jen směrnice NIS, byla vydána v roce 2016 Evropským parlamentem. Cílem je sjednocení právní úpravy členských států v oblasti bezpečnosti sítí a informačních systémů a zavedení jednotného standardu úrovně kybernetické bezpečnosti [13].

Některé povinnosti z této směrnice jsou již zaneseny do KBZ a jeho prováděcích předpisů. Z této směrnice vzešlo rozšíření okruhu subjektů povinností v oblasti ochrany a prevence před kybernetickými bezpečnostními incidenty, jde o provozovatele základní služby a poskytovatele digitálních služeb [13].

Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích

Tato vyhláška je v platnosti od roku 2014 a stanovuje významné informační systémy a kritéria pro jejich určení [13]. V příloze (Příloha 3.) je uvedeno schéma procesu určování

významných informačních systémů [14].

Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury

Toto nařízení je platné od roku 2010. Určuje kritéria pro určení prvku kritické infrastruktury. Jsou definována odvětvová a průřezová kritéria [13]. V příloze (Příloha 4.) je uvedeno schéma procesu určování prvku kritické informační infrastruktury [15].

Vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby

Tato vyhláška je z roku 2017. Autorem vyhlášky je Národní úřad pro kybernetickou a informační bezpečnost spolu s veřejností. Vyhláška upravuje kritéria pro určení provozovatele základní služby [13].

Prováděcí nařízení komise (EU) 2018/151, kterým se stanoví pravidla pro uplatňování směrnice Evropského parlamentu a Rady (EU) 2016/1148 (Směrnice NIS).

Toto nařízení specifikuje povinnosti poskytovatele digitálních služeb. Obsahuje bezpečnostní opatření a parametry významnosti dopadu incidentu pro poskytovatele digitálních služeb. Nařízení je účinné od roku 2018 [13].

Nařízení Evropského parlamentu a Rady (EU) 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)

Toto obecné nařízení představuje právní rámec ochrany osobních údajů v evropském prostoru. Jedná se o nařízení, kterému se říká GDPR. Zkratka GDPR znamená General Data Protection Regulation. Nařízení je platné od roku 2018 [16].

Díky tomuto nařízení by měly firmy při ochraně osobních údajů uvažovat o bezpečnosti již při návrhu systému na zpracování osobních údajů a měly by aplikovat taková opatření, které zaručí vysokou míru bezpečnosti těchto dat, a to z pohledu triády CIA. Společnosti budou muset mimo jiné implementovat pseudonymizaci a šifrování osobních údajů [16].

Každý občan EU tímto nařízením získal právo na opravu, na výmaz, na omezení spracování, na přenositelnost údajů, na vznesení námitky a právo nebýt předmětem žádného rozhodnutí založeného výhradně na automatickém spracování [16].

Získané vzorky, na kterých bude probíhat analýza, spadají do prvků kritické informační infrastruktury nebo jde o správce významných informačních systémů. Žádný ze vzorků není poskytovatelem základní služby nebo poskytovatelem digitální služby. Proto se těmito pojmy dále nezabýváme.

2.5 Kritická informační infrastruktura

Kritickou informační infrastrukturu definuje zákon č. 240/2000 Sb., krizový zákon. Rozumí se tím prvek nebo systém prvků kritické infrastruktury, a to v odvětví komunikačních a informačních systémů v oblasti kybernetické bezpečnosti. Dále je specifikováno v zákoně č. 181/2014 Sb., o kybernetické bezpečnosti. Jedná se tedy o informační a komunikační systémy, popřípadě ICS nebo SCADA systémy, které spadají do kritérií pro určení prvku KII. Tato kritéria jsou uvedena v nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury [13].

IS nebo KS kritické informační infrastruktury má správce, kterým je osoba nebo orgán, který udává účel komunikačního systému nebo účel zpracování informací a udává podmínky pro provozování IS nebo KS [13].

Osoba nebo orgán, který řeší funkčnost technických a programových prostředků IS nebo KS, je provozovatel IS nebo KS kritické informační infrastruktury. Správce určuje programové a technické prostředky a informuje provozovatele [13].

2.6 Významný informační systém

Významný informační systém je takový IS, který není kritickou informační infrastrukturou ani informačním systémem základní služby a u kterého by v případě narušení bezpečnosti informací (narušení triády CIA) došlo k omezení nebo ohrožení výkonu působnosti

orgánu veřejné moci, který spravuje tento systém. Významný informační systém je specifikován v zákoně č. 181/2014 Sb., o kybernetické bezpečnosti a kritéria pro rozhodnutí o VIS jsou uvedena ve vyhlášce č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích [13].

Osoba nebo orgán, určující účel zpracování informací a udávající podmínky provozování IS, je správcem významného informačního systému [13].

Provozovatel významného informačního systému zajišťuje funkčnost technických a programových prostředků, které tvoří IS. Správce tyto prostředky určuje a informuje provozovatele [13].

2.7 Systém řízení bezpečnosti informací

Systém řízení bezpečnosti informací (Information Security Management System) neboli ISMS. Jde o součást řízení organizace. Je to systém pro řízení a správu informačních aktiv, s cílem zamezit jejich možné ztrátě nebo poškození [3].

Cíl je dosahován pomocí určení aktiv, které se mají chránit, dále zvolením a řízením možných rizik bezpečnosti informací a zavedením opatření s požadovanou úrovní záruk, které jsou kontrolovány [3].

ISMS je možné zavést do celé organizace nebo jen v rámci informačního systému. Obsahuje IT bezpečnost, komunikační bezpečnost, personální bezpečnost, administrativní bezpečnost, fyzická bezpečnost, dokumentace a bezpečnostní funkce a mechanizmy [3].

Zavádění ISMS využívá principů Demingova modelu PDCA cyklu (Plan - Do - Check - Act) a má čtyři fáze. Stanovení cílů, určení rozsahu a odpovědností je první fáze. Ve druhé fázi se zavádí a provozuje ISMS, prosazují se vybraná bezpečnostní opatření. Poté se monitoruje a přezkoumává zavedené ISMS, zajišťuje se zpětná vazba a hodnocení řízení. V poslední fázi se provádí údržba a zlepšování zavedeného systému, odstraňují se slabiny [3].

Systém řízení informační bezpečnosti je zakotven v normě ISO 27001. Tu jsme zmínili již výše. Stanovuje požadavky na bezpečnost a kritéria pro certifikaci a audity.

Pokud je efektivně zavedeno ISMS, jsou plněny principy povědomí o potřebe informační bezpečnosti, je určena odpovědnost, jsou posuzována rizika a přijata opatření pro dosažení takové úrovně rizika, které jsme schopni přijmout, dále je zajištěn komplexní přístup k řízení informační bezpečnosti a dochází k neustálému vylepšování systému řízení [3].

Před začátkem zavádění ISMS je nutné, aby souhlasil vrcholový management s nasazením systému řízení. Při certifikaci je to první věc, která se kontroluje. Dokument musí vyjadřovat ochotu a vůli společnosti zavést a podporovat systém ISMS. Dále identifikujeme aktiva, provedeme jejich ocenění a vypracujeme analýzu rizik. Na analýze rizik stojí celý systém řízení bezpečnosti informací. K návaznosti na analýzu rizik vypracujeme návrh opatření, která efektivně eliminují / sníží identifikovaná rizika. Pokud je oprávnění příliš drahé a míra rizika velmi nízká, můžeme rizika akceptovat. V této části se také vypracovává Prohlášení o aplikovatelnosti, ve kterém jsou popsány cíle opatření a jednotlivá bezpečnostní opatření, které jsou pro společnost relevantní a aplikovatelná. Musí se také vytvořit dokument, který bude přesně popisovat které části ISMS a jak jsou ve firmě zavedeny. Po předchozích krocích můžeme zavedené ISMS certifikovat. Není to však povinné. Certifikuje se povinná dokumentace a poté se kontroluje praktické zavádění ISMS [3].

3 ANALÝZA PROBLÉMU A SOUČASNÉ SITUACE

V této kapitole se zaměříme na popis asistovaného zhodnocení. Také si popíšeme způsob, jakým byly získány vzorky, dále práci s daty před samotným zpracováním a co data obsahují. Rozebereme také oblasti povinností, které se v asistovaných zhodnoceních vyskytují. Uvedeme, jak takové hodnocení probíhá a co je výsledkem hodnocení.

3.1 Asistované zhodnocení

Asistované zhodnocení obsahuje zhruba 350 otázek, které jsou rozděleny do 26 oblastí. Tyto oblasti vychází ze zákonu o kybernetické bezpečnosti a z vyhlášky o kybernetické bezpečnosti. Počet otázek i oblasti se mohou měnit. Pověřená osoba, která vypracovává asistované zhodnocení, může na základě informací o společnosti vytvářet další oblasti, dělit stávající oblasti, využít pouze některé otázky apod. Aby forma asistovaných zhodnocení byla celistvá, bude uvedena metodika pro vypracování asistovaného zhodnocení.

Pověřená osoba nebo auditor provádí asistované zhodnocení přímo ve společnosti. V první řadě získá základní informace o společnosti, kde sídlí, kolik má zaměstnanců, v čem podniká, klíčové služby a ICT, outsourcing, regulace apod. Díky základním informacím si pověřená osoba zaměří oblasti, které je ve společnosti třeba probírat. Dále se určí, kdy a s kým bude asistované zhodnocení prováděno. Analytik se společností vypracuje odpovědi na otázky uvedené v asistovaném zhodnocení. Poté provede hodnocení výsledků. Výstupem pro společnost je hodnocení situace ve společnosti z oblasti bezpečnosti, dále jsou společnosti předána doporučení analytika, zjištěná rizika, místa, na která je potřeba se zaměřit při implementaci a potřebné dokumenty.

3.2 Popis dat a jejich čištění

Každý vzorek přestavuje odpovědi na otázky v dotazníku asistovaného zhodnocení nějaké společnosti. Celkem bylo dotazováno 34 společností a u každé se zodpovídalo 256 otázek. Otázky jsou členěny do 34 oblastí. Získali jsme tedy matici, která obsahuje 8704 údajů.

Nejdříve je nutné data očistit od špatných nekorektních hodnot a sjednotit jejich strukturu. Jelikož asistovaná zhodnocení vzorků nebyla prováděna jednou osobou, vznikla nesourodost formátu těchto zhodnocení. V první fázi tedy probíhala úprava těchto dat. Pro analýzu nad daty bylo potřeba sjednotit formát a strukturu dat. Bylo nutné odstranit prázdné a chybné hodnoty a opravit pořadí získaných hodnot.

Následně byl vytvořen datový soubor s proměnnými oblast, povinnost, KII, VIS, GDPR, vzorek 1-34. Data byla zpracovávána pomocí softwaru MS Excel a Minitab.

Vzorky byly získány z různých oborů podnikání a jejich velikosti jsou také různé. Společnosti jsou rozčleněny do čtyř oborů podnikání: obchod, služby, výroba a státní správa. Dále jsou také členěny dle velikosti, která je určena počtem zaměstnanců. Podařilo se také zjistit, které vzorky patří do KII a které do VIS. V návrhové části této práce se budeme snažit nalézt vlastnosti všech těchto skupin. Zanalyzujeme data z pohledu velikosti, oboru podnikání i dle toho, zda spadají do KII nebo VIS.

3.3 Podmínky pro provedení asistovaného zhodnocení

První nutnou podmínkou pro provedení asistovaného zhodnocení je souhlas vrcholového managementu s vypracováním asistovaného hodnocení. Vrcholový management musí vypracování asistovaného zhodnocení vyžadovat a podporovat. Dále je potřeba, aby spolupracovaly veškeré subjekty, které bude pověřená osoba potřebovat k vypracování asistovaného zhodnocení.

Osoba, která zpracovává asistované zhodnocení musí být k tomuto způsobilá. Je potřeba, aby měla zkušenosti z oblasti bezpečnosti a praxi v tomto oboru. Měla by znát souvislosti a provázanosti v checklistu asistovaného zhodnocení. Musí být schopna rozhodnout, dle aktuálního stavu ve sledované společnosti, zda je konkrétní povinnost nerelevantní, neaplikovaná, neaplikovatelná, aplikovaná a do jaké míry.

3.4 Části asistovaného zhodnocení

Asistované zhodnocení provádí pověřená osoba a výsledky zapisuje do tzv. checklistu, tedy tabulkového souboru v MS Excel. V tomto souboru je uvedena vždy oblast, do které spadá daná povinnost, dále pak samotná povinnost, která se hodnotí. Dalším prvkem v asistovaném zhodnocení je reference, toto pole udává normy a zákony, ze kterých vyplývá daná povinnost, nebo ve kterých je specifikována. Soubor obsahuje k některým povinnostem také nápovědu. Ta krátce popisuje, co je předmětem hodnocení u dané povinnosti. Další tři pole jsou KII, VIS a GDPR. Tato pole jsou buď prázdná a pokud nejsou, znamená to, že je daná povinnost nutná pro subjekty kritické informační infrastruktury, významné informační systémy nebo spadá do oblasti GDPR. Posledním políčkem je hodnocení, které zapisuje pověřená osoba. Hodnocení musí být jedno z pěti definovaných: nerelevantní, neaplikováno, částečně aplikováno, aplikováno a neaplikovatelné. Více o těchto hodnoceních si řekneme později.

Tabulka 1: Ukázka prvků asistovaného zhodnocení.[Zdroj: vlastní zpracování]

Oblast	Povinnost	Ref.	Nápověda	KII	VIS	GDPR
ISMS	Stanoven rozsah a hranice ISMS. (Je určeno, kterých organizačních částí a technických prvků se ISMS týká.)	VKB, § 3, odst. 1 a)	a) vymezení rozsahu ISMS (seznam aktiv a jejich vlastníků/garantů), vymezení hranic b) vymezení ROZSAHU i toho, co je z rozsahu vyloučeno c) schéma organizace, pobočky, lokality primární popis klíčových aktiv d) ujistit se, že jsou v rozsahu všechna důležitá aktiva	KII		

3.5 Jaké oblasti otázek se v použitém dotazníku vyskytují

Zde se zaměříme na oblasti povinností, které se testují při asistovaném zhodnocení. Ve sledovaných vzorcích a jejich asistovaných zhodnoceních jsme zaznamenali 34 oblastí. Tyto oblasti se však mohou různě měnit a přidávat nové přímo dle analyzovaného subjektu. Asistované zhodnocení primárně stojí na oblastech, které jsou uvedeny v této části. Tyto

oblasti vycházejí ze zákona o kybernetické bezpečnosti a z vyhlášky o kybernetické bezpečnosti.

V asistovaných zhodnoceních, která jsou použita v této práci jsou oblasti různě přizpůsobené. Jsou vytvořeny další a některé jsou shrnuty do jiné.

Obecně můžeme oblasti můžeme rozdělit do tří skupin, organizační a technické opatření a přílohy, které obsahují osobní údaje. Toto členění je dáno systémem řízení bezpečnosti informací a vyhláškou o kybernetické bezpečnosti. Níže vidíme konkrétní oblasti v jednotlivých skupinách.

Organizační opatření:

- Systém řízení bezpečnosti informací (ISMS)
- Řízení rizik
- Bezpečnostní politika
- Organizační bezpečnost
- Stanovení bezpečnostních požadavků pro dodavatele
- Řízení aktiv
- Bezpečnost lidských zdrojů
- Řízení provozu a komunikací
- Řízení přístupu a bezpečné chování uživatelů
- Akvizice, vývoj a údržba
- Zvládání bezpečnostních událostí a incidentů (incident handling)
- Řízení kontinuity činnosti (BCM)
- Kontrola a audit kybernetické bezpečnosti

Technická opatření:

- Fyzická bezpečnost
- Bezpečnost komunikačních sítí
- Správa a ověřování identit
- Řízení přístupových oprávnění

- Ochrana před škodlivým kódem
- Ochrana integrity komunikačních sítí
- Zaznamenávání událostí informačního a komunikačního systému (uživatelů a administrátorů)
- Detekce kybernetických bezpečnostních událostí
- SIEM
- Aplikační bezpečnost
- Kryptografie
- Průmyslové, řídící a obdobné specifické systémy

Přílohy:

- Osobní údaje (GDPR)

V krátkosti si přiblížíme obsah všech uvedených oblastí. Detailní rozbor najdeme v metodice pro vypracování asistovaných zhodnocení [21].

Systém řízení bezpečnosti informací vychází z PDCA cyklu (plan, do, check, act) a z normy ISO/IEC 27001, která byla popsána v předchozí kapitole. ISMS se hodnotí z pohledu zainteresovaných i externích stran. V asistovaném zhodnocení se řeší rozsah, zavádí se proces řízení rizik, tvoří se bezpečnostní politiky v oblasti ISMS a zavádí se příslušné bezpečnostní opatření. Dále se řeší monitoring a hodnocení politiky, ISMS, opatření. Hodnotí se, zda se provádí audit kybernetické bezpečnosti. Také se řeší, zda se aktualizují dokumenty a zaznamenávají se veškeré činnosti spojené s ISMS.

Řízení rizik je specifikováno v normě ISO/IEC 27005, jde však pouze o to podat informace pro zpracování řízení rizik, ne přesný postup. V této oblasti se hodnotí stanovení metodiky a dokumentace pro identifikaci, hodnocení aktiv a rizik, kritéria posuzování rizik a aktiv. Tato oblast posuzuje i to, jak se určují a posuzují hrozby a zranitelnosti, dále pak dopady na aktiva. Zda a jak se zvládají rizika, jaké jsou plány zvládání rizik, zda je zpracováno prohlášení o aplikovatelnosti nebo reaktivní a ochranná opatření se probírá také v této oblasti.

Bezpečnostní politika obsahuje pravidla, směrnice a zvyklosti, které říkají, jak se řídí, chrání a distribuují aktiva v organizaci. Bezpečnostních politik je 23. Tato oblast tedy hodnotí zavedení bezpečnostních politik a hodnocení jejich účinnosti a aktualizací.

Organizační bezpečnost je oblast, ve které se řeší zavedení organizační bezpečnosti, určení bezpečnostních rolí, výboru pro řízení kybernetické bezpečnosti nebo také odborné školení osob, zastávajících bezpečnostní role.

Stanovení bezpečnostních požadavků pro dodavatele řeší bezpečnostní opatření při smluvních vztazích. Tato část probírá také výběr dodavatelů a ustanovení ve smlouvách s dodavateli.

Řízení aktiv je zakotveno v normě ISO/IEC 27001. Tato oblast obsahuje opatření v odpovědnosti za aktiva a klasifikaci informací. Hodnotí se, zda jsou zavedena pravidla ochrany aktiv a jaká, zda jsou určení garanti aktiv apod. Identifikace a hodnocení důležitosti aktiv je také v této oblasti.

Bezpečnost lidských zdrojů řeší tři skupiny, před vznikem pracovního vztahu, během pracovního vztahu a po změně nebo zániku pracovního vztahu. Najdeme zde povinnosti týkající se školení, plánu rozvoje bezpečnostního povědomí, kontrol dodržování bezpečnostní politiky, vrácení svěřených aktiv, pravidla pro určení bezpečnostních rolí, postupů při změně postavení osob v bezpečnostních rolích apod.

Řízení provozu a komunikací je rozdělena do deseti částí. Tyto části se týkají opatření, které se snaží zajistit bezpečný provoz IS/ICT. Patří sem například zálohování informací, bezpečnost při zacházení s médii, výměna informací mezi organizací a partnery nebo služby elektronického obchodu.

Řízení přístupu a bezpečné chování uživatelů řeší přístup k informačním systémům, přihlášení uživatelů a administrátorů informačních systémů, nástroje ověřování identity, oprávnění uživatelů a přezkoumávání a kontrolu nastavení přístupových oprávnění . V této oblasti se hodnotí i bezpečné používání mobilních zařízení.

Akvizice, vývoj a údržba je oblast obsahující bezpečnostní požadavky na IS, správnost zpracování v aplikacích, kryptografická opatření v podobě správy klíčů apod., bez-

pečnost systémových souborů a procesů vývoje a podpory nebo řízení technických zranitelností.

Zvládání bezpečnostních událostí a incidentů (incident handling) obsahuje například opatření pro zajištění oznamování kybernetických bezpečnostních událostí nebo vyhodnocení oznámených kybernetických bezpečnostních událostí. Nalezneme zde i nástroje pro detekci a sběr kybernetických bezpečnostních událostí, dále klasifikaci nebo určení příčin kybernetických bezpečnostních událostí.

Řízení kontinuity činnosti (BCM) zahrnuje stanovení práv a povinností garantů aktiv, administrátorů a osob v bezpečnostních rolích, dále stanovení strategie a cílů řízení kontinuity činností, identifikace a dokumentace incidentů a rizik související s ohrožením kontinuity činností. Důležitou částí této oblasti jsou plány kontinuity činností.

Kontrola a audit kybernetické bezpečnosti posuzuje soulad bezpečnostních opatření s obecně závaznými právními předpisy, vnitřními předpisy, smluvními závazky apod. Dále se řeší dokumentace a provádění pravidelných kontrol dodržování bezpečnostní politiky, zda je proveden audit kybernetické bezpečnosti dle vyhlášky kybernetické bezpečnosti nebo zda jsou prováděny kontroly zranitelnosti technických prostředků.

Fyzická bezpečnost je oblast, která se zabývá fyzickou bezpečností perimetru, kontrolou fyzického přístupu, zabezpečené prostorů a prostředků, posuzuje vnější hrozby a vliv prostředí apod. V této oblasti najdeme také opatření pro zařízení chránící prvky infrastruktury ICT jako ochranu kabelových rozvodů, bezpečnou likvidaci nebo UPS zařízení. Ochrana zařízení i společnosti jako celku společně nesmí kolidovat, musí fungovat současně a společně. Najdeme zde také práci s nástroji pro mazání dat.

Správa a ověřování identit obsahuje povinnosti, které řeší používání nástrojů pro ověření identity, délku a složitost hesel, dobu aktualizací hesel, zamezení přístupu dříve používaných hesel apod.

Řízení přístupových oprávnění se zabývá správou přístupových oprávnění k adresářům, datům, nastavením, souborům atd. Dále je zde zahrnuto zaznamenávání použití přístupových oprávnění.

Ochrana před škodlivým kódem se zajišťuje pomocí nástrojů, které zajistí ově-

ření a stálou kontrolu komunikace mezi vnitřní a vnější sítí, serverů a sdílených úložišť a pracovních stanic. V této oblasti se řeší také pravidelná aktualizace takového nástroje.

Ochrana integrity komunikačních sítí zahrnuje především topologii sítě. Hodnotí se zde výběr topologie, možnost segmentace, filtrace a síťové prvky, které to umožňují. Do této oblasti patří nástroje jako VLAN nebo demilitarizované zóny.

Zaznamenávání událostí informačního a komunikačního systému (uživatelů a administrátorů) se provádí pomocí nástrojů pro sběr informací o provozních a bezpečnostních činnostech a pro ochranu získaných informací před neoprávněným čtením nebo změnou. Zde je velmi důležitá synchronizace jednotného systémového času, která by měla být prováděna jednou za 24 hodin.

Detekce kybernetických bezpečnostních událostí je řešena pomocí nástroje, který vychází ze stanovených bezpečnostních potřeb a výsledků hodnocení rizik. Nástroj by měl zajistit ověření, kontrolu a případné zablokování komunikace. Jako takový nástroj můžeme označit zařízení IDS.

SIEM neboli nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí se zabývá nástroji pro monitoring, ukládání a správu bezpečnostních událostí a to ve formě log záznamů. Tyto nástroje slouží pro bezpečnostní analytiky, auditory a manažery. Tato oblast hodnotí i aktualizaci nastavení pravidel pro vyhodnocování kybernetických bezpečnostních událostí nebo využívání informací získaných z nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí.

Aplikační bezpečnost obsahuje například povinnosti jako provádění bezpečnostních testů zranitelnosti aplikací nebo zajištění ochrany aplikací a informací dostupných z vnější sítě. Najdeme zde také zajištění trvalé ochrany transakcí.

Kryptografie je oblast, ve které najdeme kryptografické prostředky. Určují se zde pravidla kryptografické ochrany, úroveň kryptografické ochrany s ohledem na kryptografické algoritmy, volba prostředků pro zajištění důvěrnosti a integrity předávaných nebo ukládaných dat a prokázání odpovědnosti za provedené činnosti. V této oblasti se řeší systém správy klíčů nebo kryptografické algoritmy.

Průmyslové, řídící a obdobné specifické systémy využívají nástroje, které zajistí

omezení fyzického přístupu k síti a zařízením průmyslových a řídících systémů nebo omezení propojení a vzdáleného přístupu k síti průmyslových a řídících systémů. Hodnotíme také obnovení chodu průmyslových a řídících systémů po kybernetickém bezpečnostním incidentu.

Zajištění dostupnosti bývá řešeno pomocí záloh a redundance. Tato oblast hodnotí použití nástroje pro zajišťování dostupnosti informací, informačního systému, odolnosti informačního systému nebo zálohování technických aktiv a redundanci.

Osobní údaje jsou nejobsáhlejší oblastí. Řeší se zde identifikace osobních údajů zpracovaných organizací, opatření k zajištění úrovně zabezpečení dle GDPR v závislosti na rizicích. Dále zde nalezneme pseudonymizaci, šifrování osobních údajů, zajištění důvěrnosti, integrity, dostupnosti a odolnosti systémů a služeb zpracování osobních údajů, pravidelné testování a hodnocení účinnosti opatření apod. Tato oblast specifikuje i role správce, příjemce nebo zpracovatele dat, role DPO apod. Zaznamenávání práce s osobními daty, uchovávání dat, hromadné zpracování dat nebo zálohy jsou taktéž v této oblasti a mnoho dalšího.

Osobní údaje – kodexy chování je oblast obsahující právě kodexy chování v souvislosti se zpracováním osobních údajů, určuje se, zda a jak se dodržují schválené kodexy chování a zda má společnost vydáno osvědčení dle čl. 40 GDPR.

Osobní údaje – závazná podniková pravidla je oblast, ve které nalezneme jakousi koncepci ochrany osobních údajů. Je vymezena struktura a kontaktní údaje v hospodářském řetězci, předání údajů nebo soubor předání, právně závazná povaha apod. Omezuje se pravidly i doba uložení, kvalita údajů nebo ochrana osobních údajů.

Osobní údaje – záznamy o činnostech zpracování obsahují údaje o správci nebo zástupci a pověřenci pro ochranu osobních údajů, účely zpracování, kategorii subjektů údajů i osobních údajů nebo příjemců. Dále se hodnotí, zda se vedou záznamy o případném předání osobních údajů do třetí země nebo mezinárodní organizaci. Nebo zda jsou vedeny záznamy o všech kategoriích činností zpracování prováděných pro správce.

Osobní údaje – posouzení vlivu na ochranu osobních údajů je oblast, kde jsou povinnosti charakterizovány v podobě otázek. Například zde najdeme, zda společnost

zpracovává údaje na základě automatizovaného rozhodování, zda monitoruje adresné chování zákazníků, zda zpracovávají data o zaměstnancích nebo zda evidují údaje dle územního rozsahu.

Osobní údaje – právo na přenositelnost údajů je oblast, která není rozsáhlá. Hodnotí se zde, jak jsou data vědomě poskytnutá nebo poskytnutá zákazníkem na základě využití služby.

3.6 Kdy a proč provést asistované zhodnocení

Asistované zhodnocení doporučujeme provést v každé společnosti. Velmi žádoucí je však v případě, že společnost spadá do KII nebo VIS a potřebuje zjistit, jaká je její situace. Asistované zhodnocení je vhodné provádět také před zavedením ISMS nebo jakoukoliv bezpečnostní certifikací.

Asistované zhodnocení dá společnosti ucelený pohled na její aktuální stav v oblasti bezpečnosti. Díky tomu může odstranit své slabiny, nalézt zbytečné nebo příliš složité procesy, které ve společnosti tvoří problémy. Společnost získá zpětnou vazbu a možnost opravit a vylepšit vše, co v bezpečnosti prozatím zavedla. Asistované zhodnocení může sloužit také jako podklad pro tvorbu povinné dokumentace, například pro správce kritické informační infrastruktury nebo významných informačních systémů.

3.7 Hodnocení povinností

Asistované zhodnocení obsahuje také hodnocení každé povinnosti v něm. Osoba provádějící asistované zhodnocení má možnost uvést vždy jednu z pěti možností hodnocení: nerelevantní, neaplikováno, částečně aplikováno, aplikováno a neaplikovatelné.

Nerelevantní hodnocení se dává v případě, že danou povinnost nelze ve společnosti hodnotit nebo je pro ni zbytečná.

Hodnocení **neaplikováno** dává auditor nebo analytik, pokud alespoň část povinnosti není ve společnosti zavedena a dodržována.

Částečně aplikováno je hodnocení povinností, které jsou zavedeny ve společnosti pouze z části, nejsou plně dodržovány a realizovány, ale z velké části jsou zapracovány.

Hodnocení **aplikováno** získá společnost k dané povinnosti, pokud je plně zavedena a její princip je zcela dodržován. Musí být zavedeny vždy všechny části dané povinnosti.

Neaplikovatelné hodnocení je uděleno v případě, že povinnost nebo opatření není možné zavést. Důvodem mohou být překážky ze strany společnosti i z vnějšího okolí.

3.8 Výsledek asistovaného zhodnocení

Jak již bylo zmíněno, analytik zpracuje odpovědi na otázky dokumentu asistovaného zhodnocení, provede hodnocení a vypracuje výstupní dokumenty. Výstupem jsou následující dokumenty:

- hodnocení situace ve společnosti z oblasti bezpečnosti,
- doporučení analytika,
- zjištěná rizika,
- slabá místa,
- potřebné dokumenty.

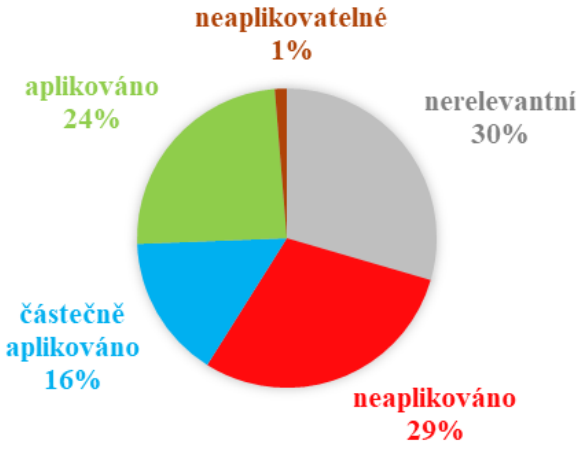
4 VLASTNÍ NÁVRHY ŘEŠENÍ, PŘÍNOS NÁVRHŮ ŘEŠENÍ

V této kapitole se budeme věnovat analýze získaných vzorků asistovaných zhodnocení. Pokusíme se nalézt vlastnosti, které by mohly být využity v praxi při provádění dalších asistovaných zhodnocení.

4.1 Souhrnné hodnocení všech vzorků

V této části zanalyzujeme všechny vzorky souhrnně. Uvedeme celkové hodnocení všech vzorků a dále se zaměříme na vzorky, které nějakým způsobem vynikají.

Graf (Graf 1.) níže zobrazuje výsledky všech asistovaných zhodnocení dohromady. Jak můžeme vidět, 30 % hodnot je nerelevantních. To znamená, že pro dané společnosti nemá smysl uvažovat 30 % povinností.



Graf 1: Souhrnné hodnocení všech vzorků.[Zdroj: vlastní zpracování]

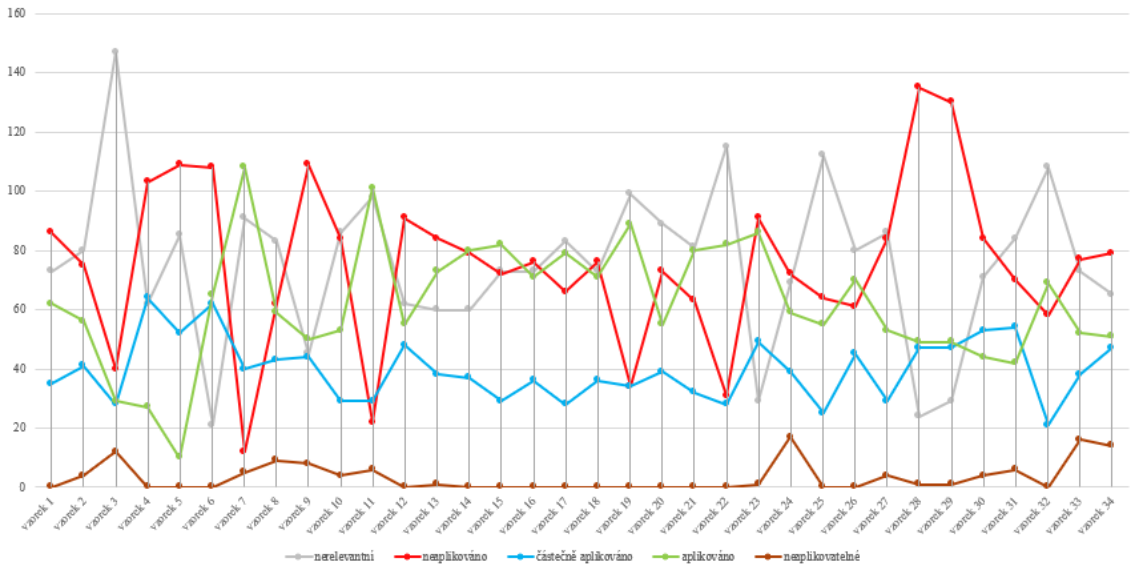
Neaplikovatelných povinností je pouze 1 %. Neaplikovaných je však velice vysoký podíl, celkem 29 % povinností společnosti prozatím nemají aplikovány. O něco nižší podíl mají aplikované povinnosti, 24 % a celkem 16 % povinností je částečně aplikováno. V dalším grafu (Graf 2.) je zobrazen výsledek při vynechání všech nerelevantních hodnot. Zde je vidět, že skoro polovina povinností není aplikována. Aplikovaných povinností je

34 % a částečně aplikovaných je 22 %.

Graf 2: Souhrnné hodnocení relevantních hodnot.[Zdroj: vlastní zpracování]

Průměrný počet nerelevantních povinností je 76, což je 30 %. Celkem 29 % povinností je průměrně neaplikovaných, 15 % je v průměru částečně aplikováno, 24 % tedy 62 povinností je průměrně aplikováno zcela a pouhé 1 % je v průměru neaplikovatelné.

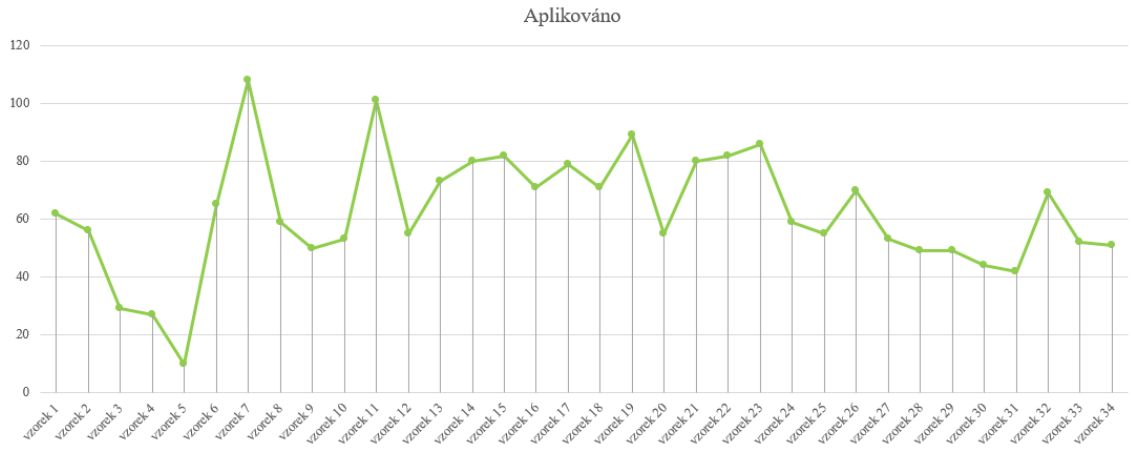
Nyní se podíváme na jednotlivé kategorie z pohledu všech vzorků. Následující graf (Graf č. 3) znázorňuje počty jednotlivých hodnocení dle všech vzorků.



Graf 3: Spojnicový graf všech hodnocení vzorků.[Zdroj: vlastní zpracování]

Graf (Graf č. 4) níže zobrazuje počty aplikovaných povinností u každého sledovaného vzorku. Nejhůře je na tom společnost, která odpovídá vzorku č. 5. Tento vzorek má nejméně aplikovaných povinností. Jde o společnost střední velikosti, to znamená, že má 50–100 zaměstnanců. Tato společnost podniká v oblasti služeb. Obdobně jsou na tom vzorky č. 3 a č. 4., oba vzorky spadají do skupiny mikropodniků (do 10 zaměstnanců). Vzorek č. 3 podniká také ve službách a vzorek č. 4 patří do státní správy.

Naopak nejlépe je na tom společnost, která odpovídá vzorku č. 7. Tato společnost má 100–200 zaměstnanců a jde o služby. Jen o něco méně aplikovaných povinností má vzorek č. 11. Jedná se o drobnou společnost s 10–25 zaměstnanci podnikající ve výrobě. Ostatní vzorky jsou na tom velice podobně, co se aplikovaných povinností týče. Průměrný počet aplikovaných povinností je 62.

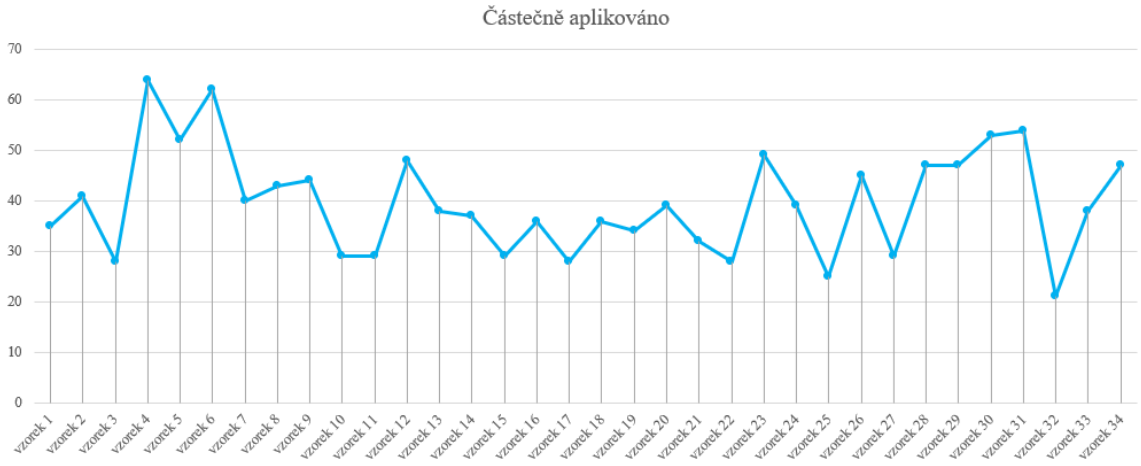


Graf 4: Spojnicový graf aplikovaných povinností.[Zdroj: vlastní zpracování]

Následující graf (Graf č. 5) popisuje počty částečně aplikovaných povinností u jednotlivých vzorků. Zde můžeme vidět, že jsou rozdíly mezi vzorky mnohem nižší než u předchozího grafu. Hodnoty se pohybují převážně okolo 40, což je také průměrná hodnota.

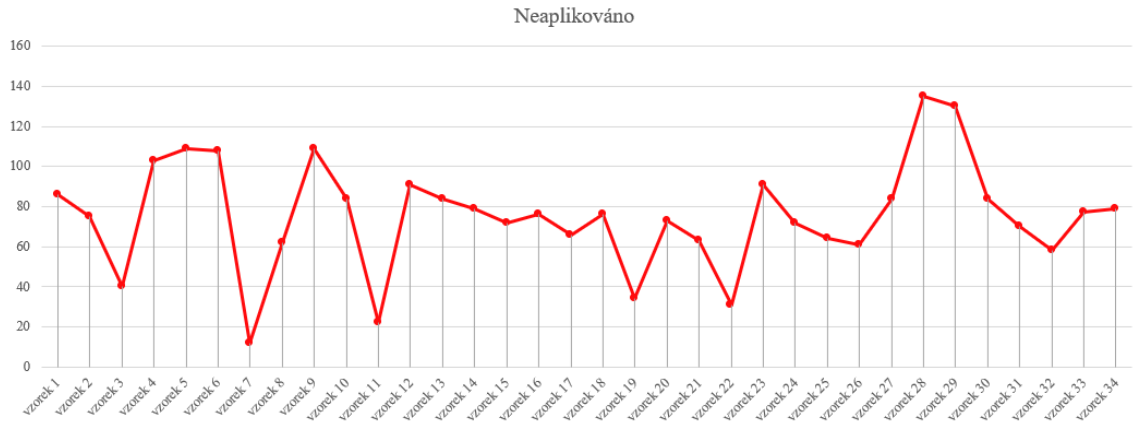
Nejvíce částečně aplikovaných povinností mají vzorky č. 4 a č. 6. Vzorek č. 4 je mikropodnikem (do 10 zaměstnanců) a patří do státní správy. Vzorek č. 6 je velkou společností (nad 500 zaměstnanců) a podniká ve výrobě. Nejméně částečně aplikovaných povinností mají pak vzorky č. 25 a č. 32. Vzorek č. 25 je větší výrobní společností (200–

500 zaměstnanců). Vzorek č. 32 je menší společnost (25–50 zaměstnanců) podnikající v oblasti obchodu.



Graf 5: Spojnicový graf částečně aplikovaných povinností.[Zdroj: vlastní zpracování]

Nejvíce nás zajímají neaplikované povinností. Jednotlivé vzorky a počty neaplikovaných povinností je vidět na grafu (Graf č. 6) níže. Největší počet neaplikovaných povinností mají společnosti, které odpovídají vzorkům č. 29 a č. 30. Oba tyto vzorky patří do státní správy. Vzorek č. 29 je společností se 100–200 zaměstnanci. Vzorek č. 30 je drobnou společností (10–25 zaměstnanců).



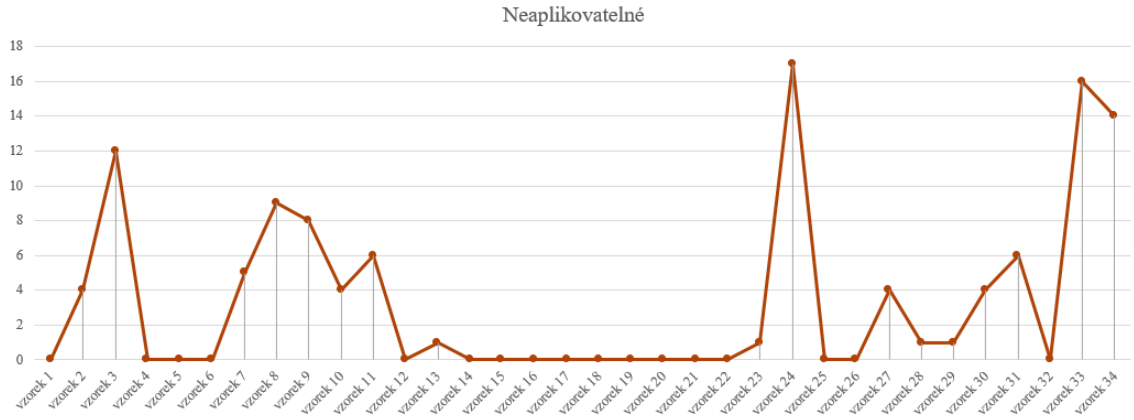
Graf 6: Spojnicový graf neaplikovaných povinností.[Zdroj: vlastní zpracování]

Naopak nejlépe na tom jsou společnosti, které patří ke vzorkům č. 7 a č. 11. Jak už bylo zmíněno výše, vzorek č. 7 je společnost se 100–200 zaměstnanci a jde o služby.

Vzorek č. 11. je drobnou společnost s 10–25 zaměstnanci podnikající ve výrobě. Lépe jsou na tom také vzorky č. 19, č. 23 a č. 3. Vzorek č. 19 je drobnou (10–25 zaměstnanců) společností a vzorek č. 23 je větší společnost (200–500 zaměstnanců). Vzorek č. 3 patří do mikropodniků (do 10 zaměstnanců). Všechny tyto tři vzorky se pohybují ve službách.

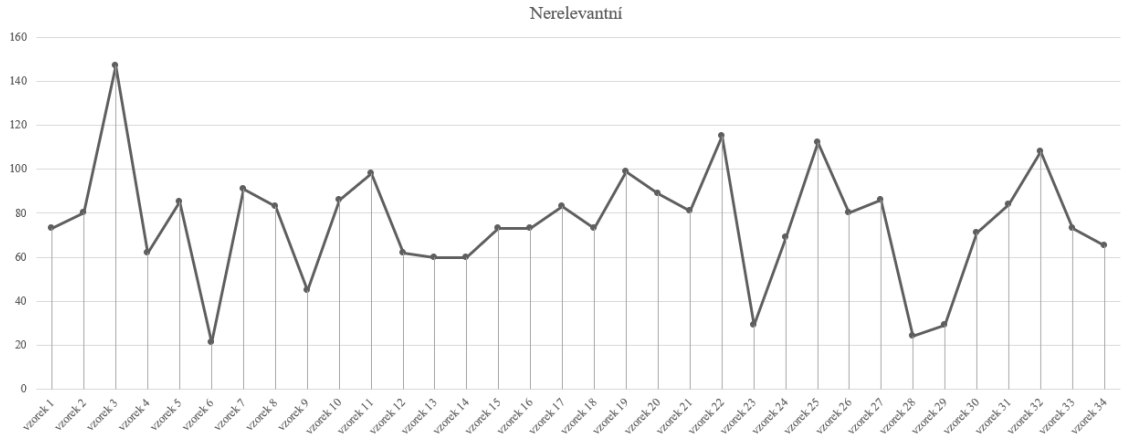
Z grafu je také vidět, že až na zmíněných několik společností jsou na tom vesměs podobně. Většinou se počet neaplikovaných povinností pohybuje okolo 70. Průměrný počet neaplikovaných povinností je 75.

Další graf (Graf č. 7) popisuje neaplikovatelné povinnosti. Zde můžeme vidět, že společnosti mají spíše nulový počet takových řešení nebo naopak vyšší. Nejvyšší počet mají vzorky č. 24, č. 33 a č. 34. Vzorky č. 24 a č. 33 spadají do státní správy a jde o střední podniky (50–100 zaměstnanců). Vzorek č. 34 je mikropodnik (do 10 zaměstnanců) podnikající ve službách. Průměrný počet neaplikovatelných povinností je 3.



Graf 7: Spojnicový graf neaplikovatelných povinností.[Zdroj: vlastní zpracování]

Poslední graf (Graf č. 8) tohoto typu znázorňuje počty nerelevantních povinností u jednotlivých vzorků. Zde můžeme vidět, že největší počet nerelevantních řešení má vzorek č. 3. Vzorek č. 3 patří do mikropodniků (do 10 zaměstnanců) pohybující se ve službách. Naopak nejmenší počet je u vzorku č. 6 a č. 28. Vzorek č. 6 je velkou společností (nad 500 zaměstnanců). Vzorek č. 28 je drobnou společností (10–25 zaměstnanců). Tyto dvě společnosti jsou výrobními podniky. Průměrný počet nerelevantních řešení je 75.



Graf 8: Spojnicový graf nerelevantních povinností.[Zdroj: vlastní zpracování]

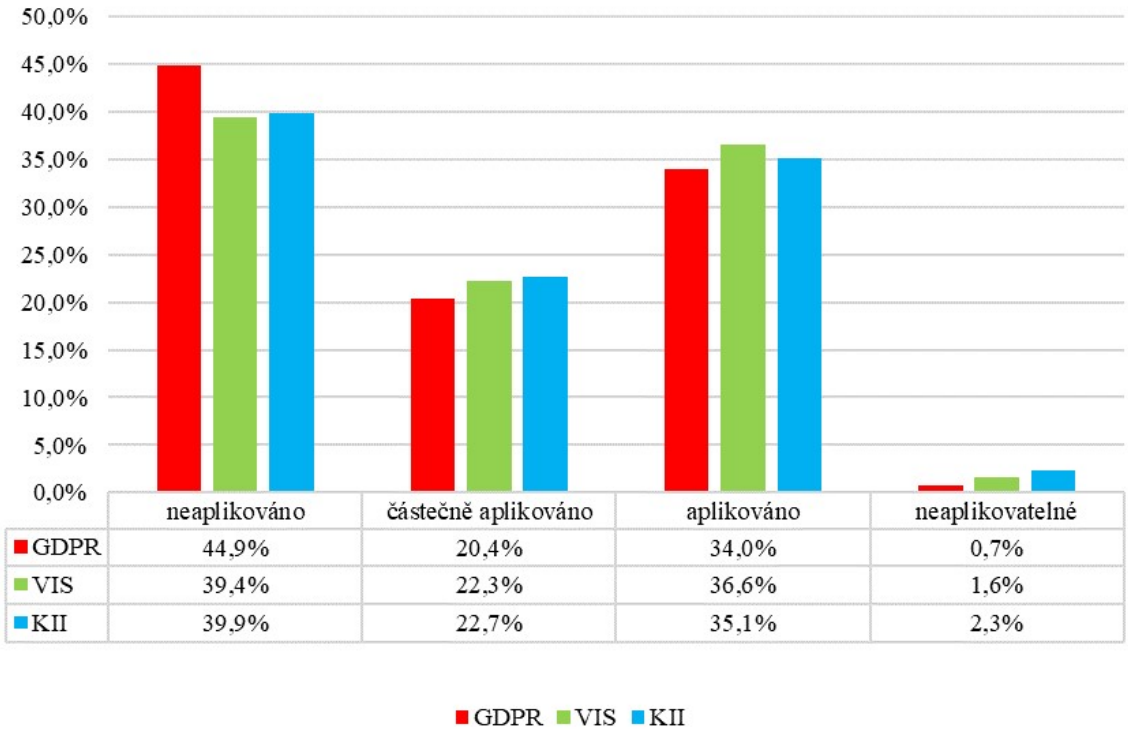
4.2 Pohled na data dle KII, VIS a GDPR

Některé oblasti jsou povinni implementovat správci informačních nebo komunikačních systémů KII, správci VIS a některé oblasti se týkají GDPR. Tyto oblasti se však často kryjí. To například znamená, že je jsou povinni implementovat jak správci KII, tak VIS. V této části se podíváme na data z těchto úhlů. Kolik povinností je v každé skupině popisuje následující tabulka (Tabulka 2.).

Tabulka 2: Počty povinností v GDPR, VIS a KII.[Zdroj: vlastní zpracování]

Skupina	Počet povinností
GDPR	80
VIS	91
KII	170

Graf (Graf 9.) níže zobrazuje výsledky vzorků pro skupiny oblastí GDPR, KII a VIS. Jelikož jsou v jednotlivých oblastech různé počty povinností, jsou hodnoty převedeny na procenta, abychom je mohli mezi sebou porovnávat. Pro správné porovnání jsou vynechány hodnoty nerelevantních povinností.



	neaplikováno	částečně aplikováno	aplikováno	neaplikovatelné
GDPR	44,9%	20,4%	34,0%	0,7%
VIS	39,4%	22,3%	36,6%	1,6%
KII	39,9%	22,7%	35,1%	2,3%

Graf 9: Porovnání oblastí KII, GDPR a VIS.[Zdroj: vlastní zpracování]

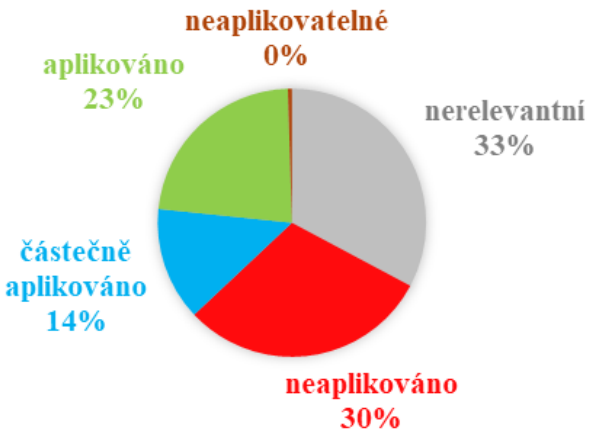
Jak můžeme vidět na první pohled vypadají hodnoty dost podobně. Celkem 58,9 % povinností aplikují zcela nebo částečně správci VIS. V této oblasti je také nejméně neaplikovaných povinností. Dalo by se říci, že správci VIS jsou nejvíce důslední v plnění povinností specifických pro jejich oblast a aplikují požadované povinností spíše než správci KII. Rozdíly však nejsou nijak markantní. Naopak oblast GDPR dělá společnostem velké potíže. Celkem 44,9 % povinností z této oblasti není aplikovaných a pouze 54,4 % je částečně nebo zcela aplikovaných.

Dále se zaměříme na každou z oblastí. Podíváme se na několik povinností, které mají společná hodnocení u více sledovaných firem. U oblastí KII a VIS se zaměříme i na konkrétní společnosti, které do těchto oblastí spadají. Zhodnotíme tyto oblasti z pohledu všech 34 vzorků i z pohledu konkrétních firem, které spadají do dané oblasti.

Obecné nařízení o ochraně osobních údajů (GDPR)

Níže můžeme vidět dva grafy. První graf (Graf 10.) popisuje relativní četnosti všech hodnocení. Druhý graf (Graf 11.) obsahuje hodnocení bez všech nerelevantních hod-

not. V části spadající do GDPR je celkem 33 % nerelevantních hodnot u analyzovaných vzorků.



Graf 10: Četnosti hodnocení v oblasti GDPR.[Zdroj: vlastní zpracování]

Nyní můžeme vidět (Graf č. 11), že v oblasti GDPR je 45 % neaplikovaných povinností. Celkem 27 společností má problém s rolí příjemce dat v oblasti osobních údajů, tyto společnosti ji nemají specifikovanou. 27 společností také neplánuje zavést pravidelná školení pro práci s osobními daty.

Graf 11: Četnosti hodnocení v oblasti GDPR (relevantní).[Zdroj: vlastní zpracování]

Celkem 26 ze sledovaných 34 společností nepoužívá šifrování osobních údajů při jejich zpracování a vůbec neřeší smluvně dodavatelský řetězec, nezajišťují tedy bezpečnost svých dat u svých dodavatelů. Dále 25 vzorků nevede záznamy o činnostech zpracování

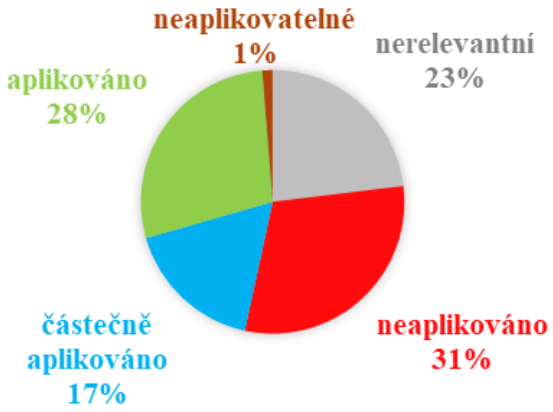
osobních údajů a nemají specifikovanou roli správce dat.

Aplikovaných povinností je celkem 34 %. Celkem 31 společnosti disponuje s papírovými osobními údaji a přistupuje k nim jako ke strojovým. Stejný počet společností má aplikované povinností ve vstupních informacích osobních údajů v personalistice, mají zpracovanou kompletní přijímací dokumentaci. 30 vzorků při zpracování osobních údajů zajišťuje schopnost obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů.

Neaplikovatelné povinnosti jsou zde ve velmi malé míře, pouze 0,7 %. Pouhé dvě společnosti nezpracovávají kodexy chování v souvislosti se zpracováním osobních údajů a nemohou aplikovat dodržování schváleného kodexu chování.

Významné informační systémy (VIS)

První graf (Graf č. 12) nám opět ukazuje všechna hodnocení. V povinnostech týkajících se významných informačních systémů je celkem 23 % nerelevantních.



Graf 12: Četnosti hodnocení v oblasti VIS.[Zdroj: vlastní zpracování]

V dalším grafu (Graf č. 13) opět vidíme hodnocení již bez nerelevantních hodnot. Celkem 32 firem v rámci kontroly a auditu neposuzuje soulad bezpečnostních opatření s předpisy společnosti a dalšími jinými předpisy vztahující se ke kybernetické bezpečnosti a určují opatření pro jejich prosazování. Dalších 30 firem nestanovuje plán rozvoje bezpečnostního povědomí v rámci bezpečnosti lidských zdrojů. Celkem 30 společností také nepoužívá kryptografickou ochranu v bezpečnostní politice.

Kromě jednoho vzorku všechny provádí pravidelné aktualizace nástrojů pro ochranu před škodlivým kódem, jejich definic a signatur. Dále 31 společností používá nástroj pro řízení přístupových oprávnění pro přístup k jednotlivým aplikacím a datům. Stejný počet firem používá také nástroj pro ochranu před škodlivým kódem, který zajistí ověření a stálou kontrolu nad komunikací mezi vnitřní sítí a vnější sítí.

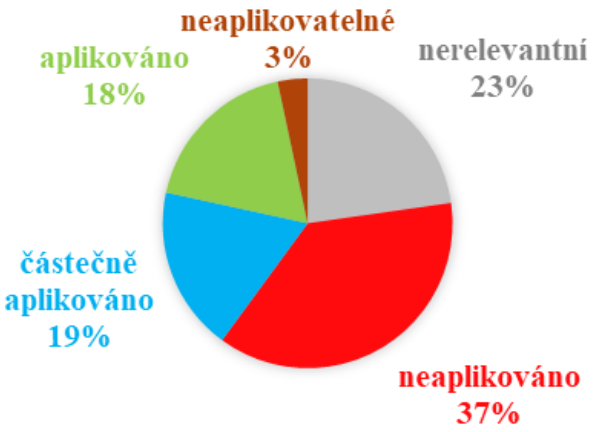
Neaplikovatelné povinnosti jsou zde opět v malé míře, celkem 1,6 %. Celkem 5 ze sledovaných společností nemůže aplikovat zaznamenávání přístupů k záznamům o činnostech, pokusy o manipulaci se záznamy o činnostech a změny, pomocí nástroje pro zaznamenávání činnosti informačního/komunikačního systému v rámci log managementu. Další 4 společnosti nemohou stanovit bezpečnostní požadavky na změny ICT spojené s jejich akvizicí, vývojem a údržbou a zahrnout je do projektu akvizice, vývoje a údržby systému. Dále u 4 firem není možné používat nástroj pro detekci kybernetických bezpečnostních událostí, který vychází ze stanovených bezpečnostních potřeb a výsledků hodnocení rizik a který by zajistil ověření, kontrolu a případné zablokování komunikace mezi vnitřní komunikační sítí a vnější sítí. U 4 firem také nelze stanovit bezpečnostní politiku ISMS nebo stanovit pravidla ochrany, která jsou nutná pro zabezpečení jednotlivých úrovní aktiv.

Graf 13: Četnosti hodnocení v oblasti VIS (relevantní).[Zdroj: vlastní zpracování]

Vzorky spadající do VIS

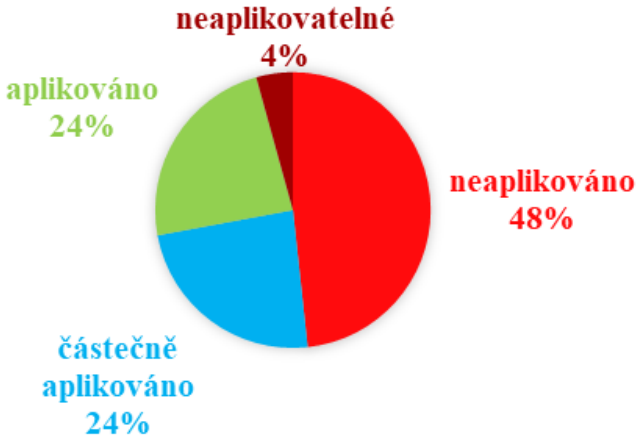
Společnosti, které spravují významné informační systémy jsou vzorky č. 4, 24, 29

a 33. V této části si zobrazíme hodnocení všech sledovaných povinností těchto vzorků (Graf 14.). Sledujeme tedy všech 256 povinností a jejich hodnocení. Zde je skoro čtvrtina všech povinností pro VIS vzorky nerelevantní.



Graf 14: Četnosti hodnocení povinností vzorků VIS.[Zdroj: vlastní zpracování]

Vynecháme nerelevantní hodnoty a zaměříme se na zbylá hodnocení plnění povinností (Graf č. 15). Podniky spadající do VIS nemají aplikováno 48 % relevantních povinností, tedy skoro polovinu povinností neaplikují. Aplikují pouze 24 % povinností a stejné množství povinností aplikují pouze částečně. Celkem 4 % řešení je však zcela neaplikovatelných.



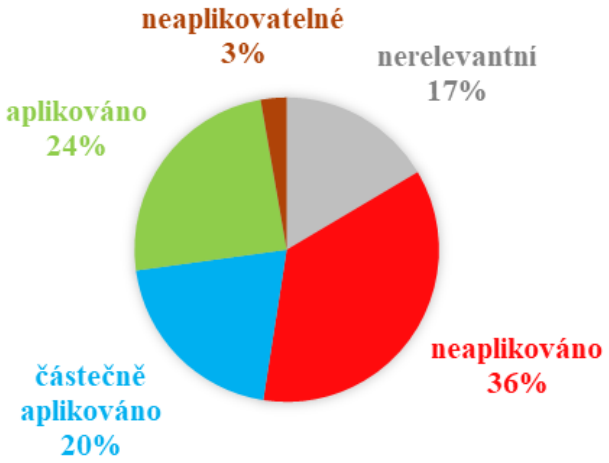
Graf 15: Četnosti hodnocení povinností vzorků VIS (relevantní).[Zdroj: vlastní zpracování]

Sledované vzorky spadající do skupiny VIS mají problém s oblastmi Řízení rizik,

Řízení dodavatelů, Bezpečnost lidských zdrojů, Kontrola a audit, OÚ - závazná podniková pravidla. V těchto oblastech jsme nalezli několik povinností, které neaplikuje ani jedna ze sledovaných firem spadajících do VIS. Velký počet neaplikovaných povinností je také v oblastech Řízení provozu a komunikací, Osobní údaje nebo Kryptografie.

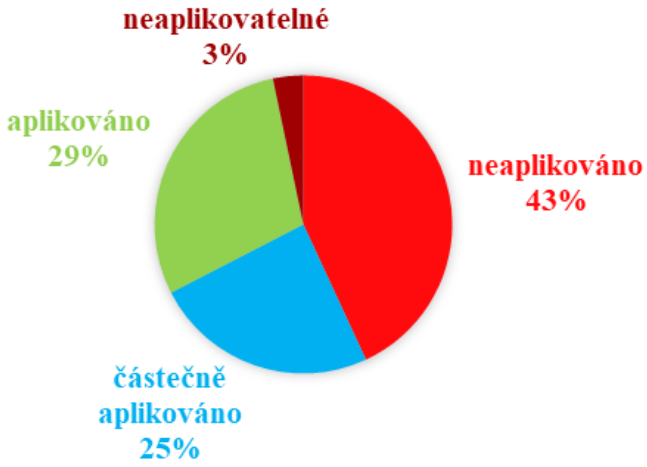
Tato skupina vzorků nemá žádnou oblast, ve které by aplikovala větší množství povinností. Pouze 9 povinností ze všech 256 jsou aplikovány u všech čtyř společností a pouze 3 povinnosti jsou u všech aplikovány částečně. Tyto společnosti se tedy dost liší a často aplikují jiné povinnosti.

Další graf (Graf č. 16) popisuje už pouze hodnocení plnění povinností vztahující se k VIS, sledujeme tedy hodnocení 91 povinností. Zjišťujeme jak podniky patřící do VIS plní povinnosti, které jsou určené přímo pro ně. Nejčastějším hodnocením VIS povinností je neaplikováno. Průměrně se však u těchto povinností využívalo hodnocení částečně aplikováno. Celkem 17 % z těchto povinností je pro vybrané vzorky nerelevantních.



Graf 16: Četnosti hodnocení VIS povinností vzorků VIS.[Zdroj: vlastní zpracování]

Když opomeneme nerelevantní povinnosti, vidíme výsledné četnosti hodnocení sledovaných vzorků níže (Graf č. 17). Zjištěné hodnoty jsou velice překvapivé. Celkem 43 % relevantních VIS povinností není u sledovaných vzorků aplikovaných. To znamená, že společnosti VIS neaplikují skoro polovinu povinností, které jsou přímo pro ně určené. Aplikují 29 % povinností a 25 % pouze částečně. Dokonce z povinností, které by vzorky spadající do VIS měly plnit, jsou 3 % povinností neaplikovatelné.



Graf 17: Četnosti hodnocení relevantních VIS povinností vzorků VIS.[Zdroj: vlastní zpracování]

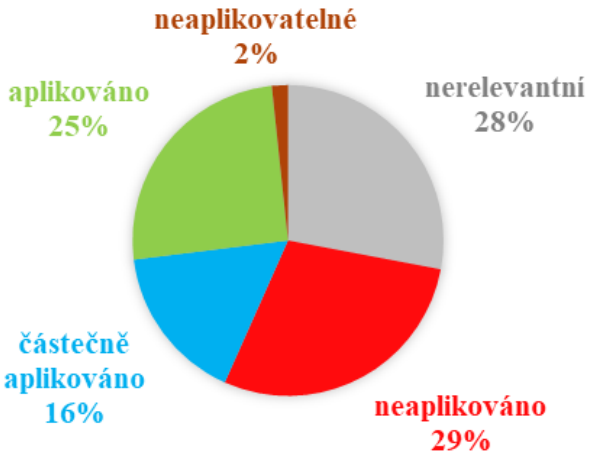
Nejhůře ze sledovaných vzorků VIS dopadl vzorek č. 29. Neaplikuje téměř polovinu relevantních povinnosti, které se týkají VIS. Aplikuje pouze 22 % plně a 28 % částečně. Jde o podnik státní správy, který má 100–200 zaměstnanců.

Nejlépe je na tom vzorek č. 24. Tato společnost aplikuje 39 % relevantních povinností z oblasti VIS, dále 18 % aplikuje částečně. Jedná se o střední společnost (50–100 zaměstnanců) patřící opět do státní správy.

Když budeme brát v úvahu pouze povinnosti, které se týkají VIS, tak všechny čtyři sledované vzorky neaplikují polovinu povinností v oblasti Řízení rizik a žádnou povinnost z oblasti Kontroly a auditu. Problémová je také oblast Bezpečnosti lidských zdrojů a Kryptografie. Na druhou stranu tyto vzorky často aplikují povinnosti v oblasti Log managementu nebo Ochrany před škodlivým kódem. Pouhé 4 povinnosti jsou u dvou firem neaplikovatelné a 2 povinnosti u jedné společnosti. Celkem existuje tedy 6 povinností, které není možné aplikovat u některých vzorků.

Kritická informační infrastruktura (KII)

V následujícím grafu (Graf č. 18) můžeme vidět podíly jednotlivých hodnocení v oblasti povinností spadajících do kritické informační infrastruktury. Zde je nerelevantních hodnot celkem 28 %.



Graf 18: Četnosti hodnocení v oblasti KII.[Zdroj: vlastní zpracování]

Dále již opět vidíme (Graf č. 19) počty hodnocení povinností bez nerelevantních hodnot. Zde se nejčastější povinnosti velice kryjí s povinnostmi v oblasti VIS. Celkem 30 firem nestanovuje plán rozvoje bezpečnostního povědomí (již jsme zaznamenali výše) a nehodnotí jeho účinnost, dále nepoužívají kryptografickou ochranu.

Graf 19: Četnosti hodnocení v oblasti KII (relevantní).[Zdroj: vlastní zpracování]

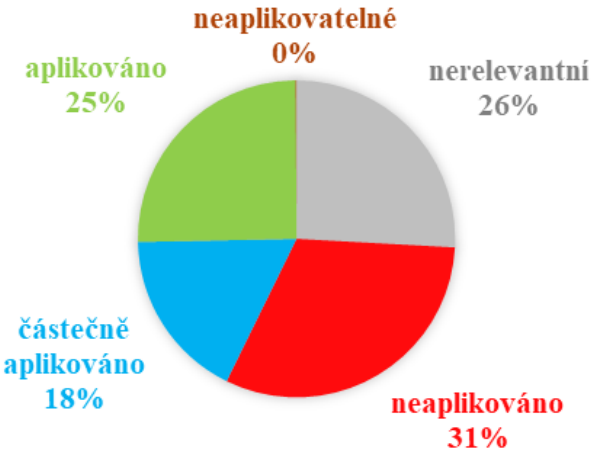
Celkem 33 společností provádí pravidelné aktualizace nástrojů pro ochranu před škodlivým kódem, jejich definic a signatur. Dále 31 firem používá nástroj pro řízení přístupových oprávnění a přiděluje přistupujícím aplikacím samostatný identifikátor.

Neaplikovatelných povinností v oblasti KII u sledovaných vzorků je celkem 2,3 %.

Povinnost, kterou nemůže aplikovat 5 firem, je společná pro oblast VIS (již bylo zaznamenáno dříve). Dále 4 společnosti nejsou schopny zajistit bezpečnost vývojového prostředí a zároveň zajistit ochranu používaných testovacích dat.

Vzorky spadající do KII

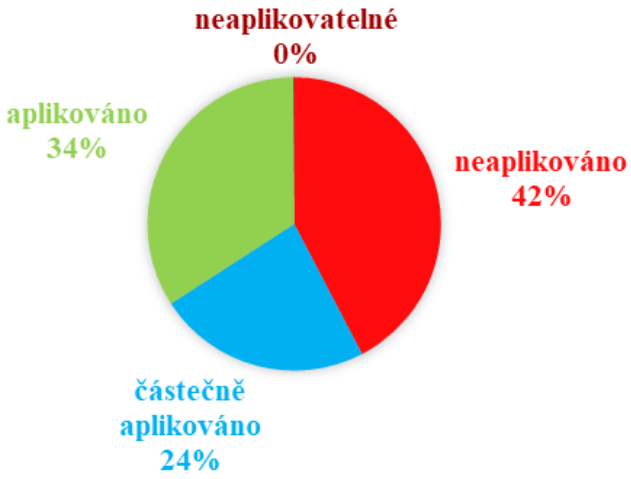
Mezi společnosti kritické informační infrastruktury patří vzorky č. 5, 6, 21, 22, 23. Nyní se podíváme, jak tyto společnosti plní své povinnosti v bezpečnosti. Následující graf (Graf č. 20) ukazuje tedy procenta hodnocení všech 256 povinností. O málo více než čtvrtina povinností je pro společnosti spadající do kritické informační infrastruktury nerelevantní.



Graf 20: Četnosti hodnocení povinností vzorků KII.[Zdroj: vlastní zpracování]

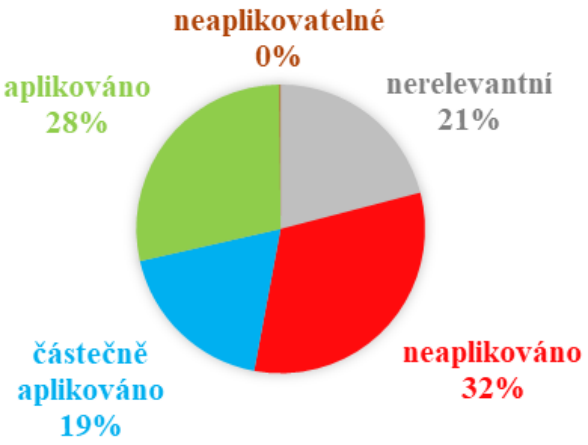
Opět vynecháme nerelevantní hodnoty a zaměříme se na zbylá hodnocení plnění povinností. Společnosti, které patří do KII nemají aplikováno 42 % relevantních povinností. Aplikují 34 % povinností a 24 % pouze částečně.

U vzorků, patřícím do kritické informační infrastruktury, jsou problémové oblasti Kryptografie, Řízení rizik a ISMS. V těchto oblastech najdeme větší množství neaplikovaných povinností. Vzorky naopak aplikují ve větší míře povinnosti z oblastí Fyzické bezpečnosti nebo Ochrany před škodlivým kódem.



Graf 21: Četnosti hodnocení relativních povinností vzorků KII.[Zdroj: vlastní zpracování]

Tento graf (Graf č. 22) popisuje už pouze hodnocení plnění povinností vztahující se ke KII, sledujeme tedy hodnocení 170 povinností. Zjišťujeme tedy jak společnosti patřící do KII plní povinnosti, které jsou určené přímo pro ně. Nejčastějším hodnocením KII povinností je neaplikováno. Průměrně se však u těchto povinností využívalo hodnocení částečně aplikováno. Celkem 21 % z těchto povinností jsou pro vybrané vzorky nerelevantní.



Graf 22: Četnosti hodnocení KII povinností vzorků KII.[Zdroj: vlastní zpracování]

Pokud vynecháme nerelevantní povinnosti, vidíme výsledné četnosti jednotlivých hodnocení níže (Graf č. 23). Zjištěné hodnoty jsou překvapující. Až 41 % relevantních KII povinností není u sledovaných vzorků aplikovaných. To znamená, že společnosti kritických informačních infrastruktur neaplikují skoro polovinu povinností, které jsou přímo pro ně určené. Aplikují 36 % povinností a 23 % pouze částečně.

Graf 23: Četnosti hodnocení relevantních KII povinností vzorků KII.[Zdroj: vlastní zpracování]

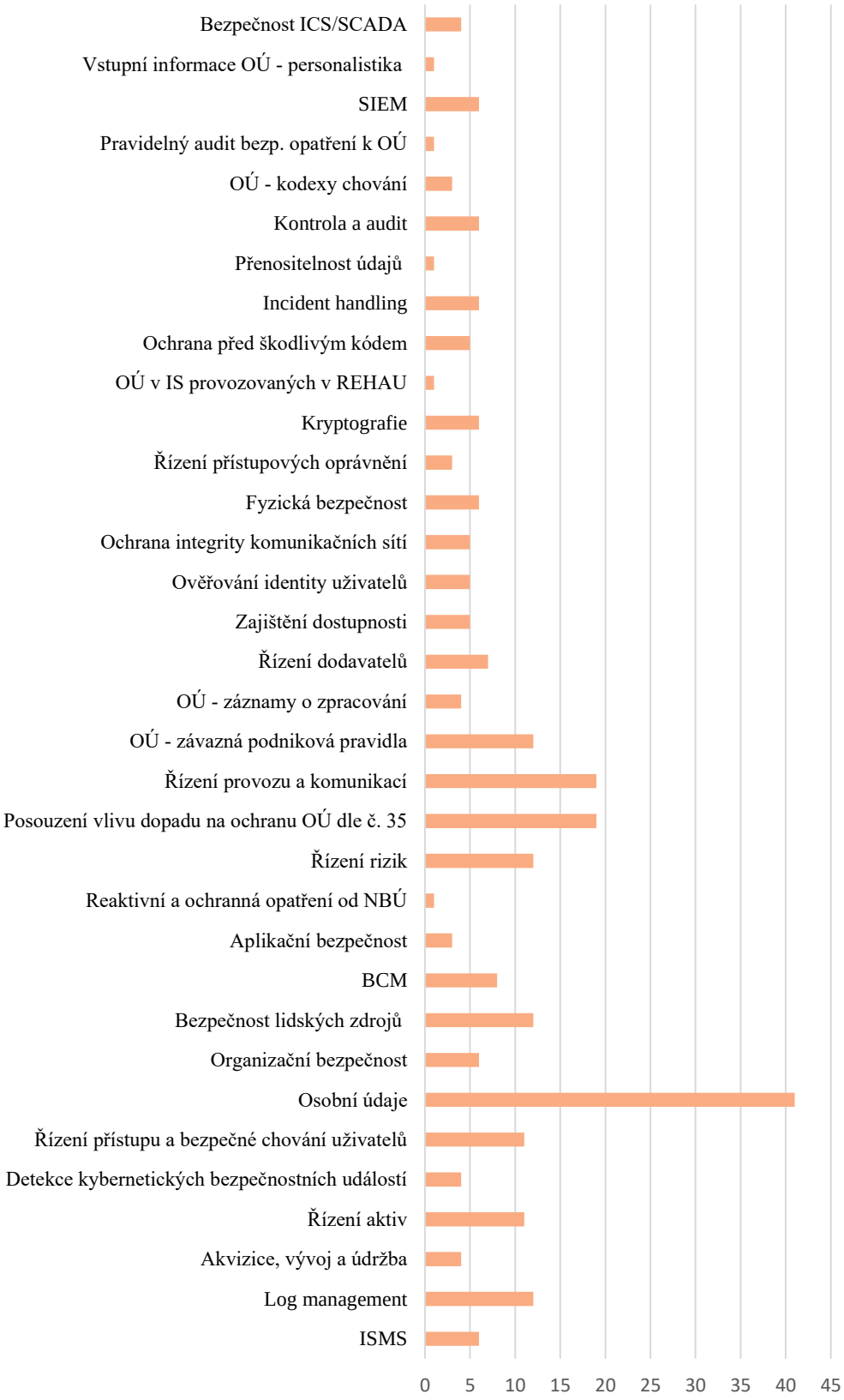
Nejhůře je na tom vzorek č. 5. Tato společnost neaplikuje 57 % povinností, které jsou pro ni relevantní a spadají do KII. Naopak aplikuje pouhých 7 % těchto povinností a 36 % aplikuje částečně. Jde o střední společnost (50–100 zaměstnanců) podnikající ve službách.

Nejlepší hodnocení ze vzorků spadajících do KII má vzorek č. 22. Tento podnik má sice dvakrát více nerelevantních povinností, ale ze zbylých relevantních KII povinností jich aplikuje 66 % a 16 % aplikuje částečně. Pouhých 18 % relevantních KII povinností tento vzorek neaplikuje. Jedná se o drobný podnik (10–25 zaměstnanců) ve státní správě.

Zaměříme se tedy na povinnosti, které se týkají KII. Velké množství povinností týkajících se KII nemají společnosti aplikovány v oblastech Kryptografie, Řízení rizik a ISMS. Těmto vzorkům však nedělá problém aplikování povinností z Fyzické bezpečnosti a Ochrany před škodlivým kódem. Pouze 1 povinnost není u jedné z těchto společností aplikovatelná. Jedná se o povinnost z oblasti Log managementu.

4.3 Pohled na data dle oblastí povinností

V asistovaném zhodnocení, které vyplňovaly společnosti s pověřenou osobou, bylo celkem 256 otázek, které odpovídají určitým povinnostem. Tyto otázky spadají do 34 oblastí. Graf (Graf 24.) ukazuje počty jednotlivých povinností (otázek) v každé z oblastí.



Graf 24: Počty otázek v jednotlivých oblastech.[Zdroj: vlastní zpracování]

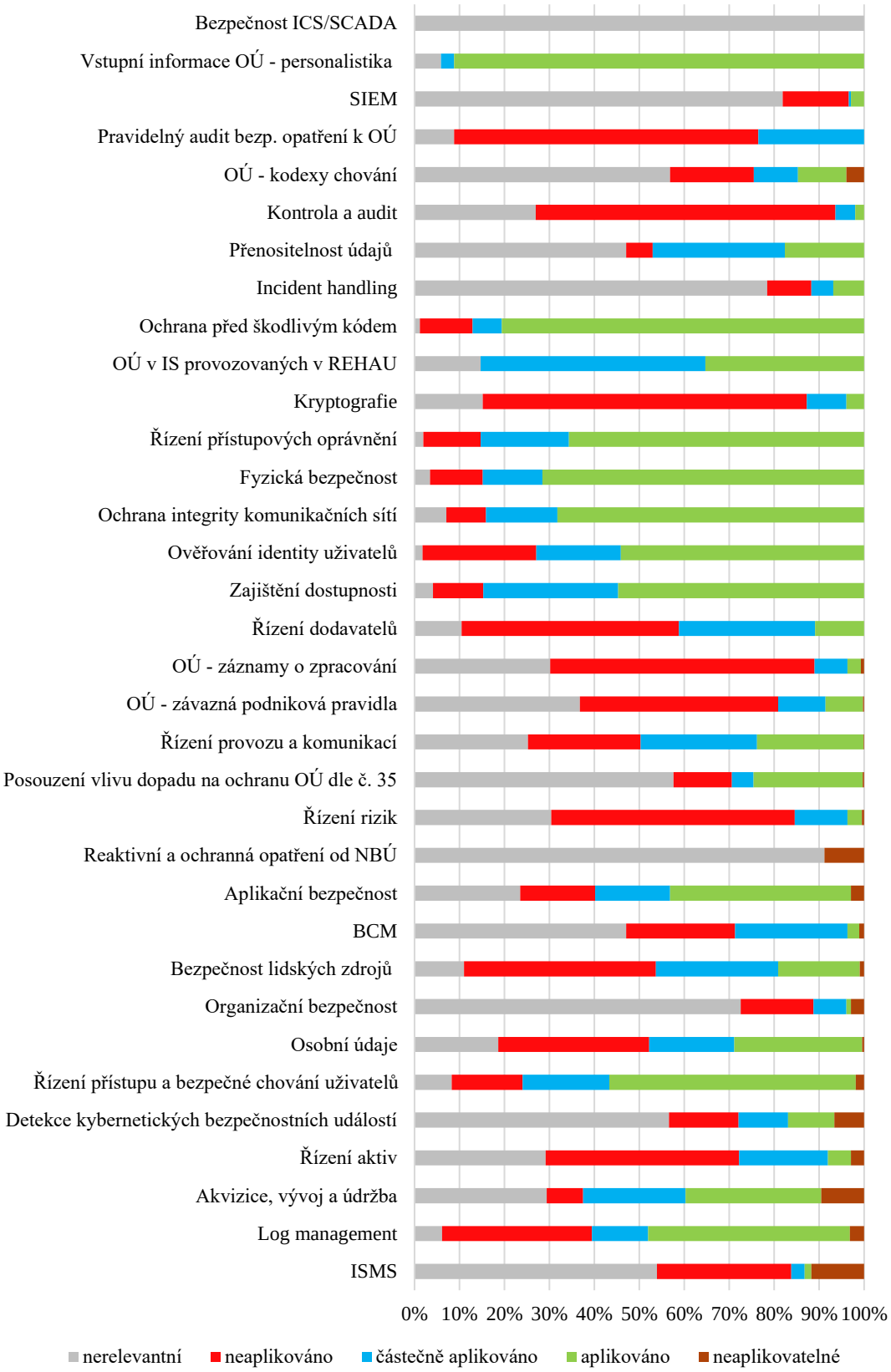
Jak můžeme vidět, nejobsáhlejší oblastí jsou Osobní údaje. Tato oblast tvoří 16 % ze všech otázek. Další oblasti zabírají 7 % a méně. Navíc jsou osobní údaje zahrnuty v mnoha dalších okruzích otázek. Například okruh OÚ - kodexy chování, OÚ - záznamy o zpracování apod. Pokud shrneme všechny otázky týkající se osobních údajů, je jich 80, což je 31 % ze všech otázek asistovaného zhodnocení, které bylo použito u dotazovaných společností.

Následují dva grafy, které zobrazují četnosti hodnocení v jednotlivých oblastech povinností. První graf (Graf 25.) ukazuje procenta hodnocení povinností v jednotlivých oblastech. Z grafu vidíme, že největší počet nerelevantních povinností je v oblasti Bezpečnost ICS/SCADA. Sledované vzorky tuto oblast nevyužívají vůbec. Dále velmi vysoký počet nerelevantních povinností je v oblastech Reaktivní a ochranná opatření od NBÚ, SIEM, Incident handling, Organizační bezpečnost.

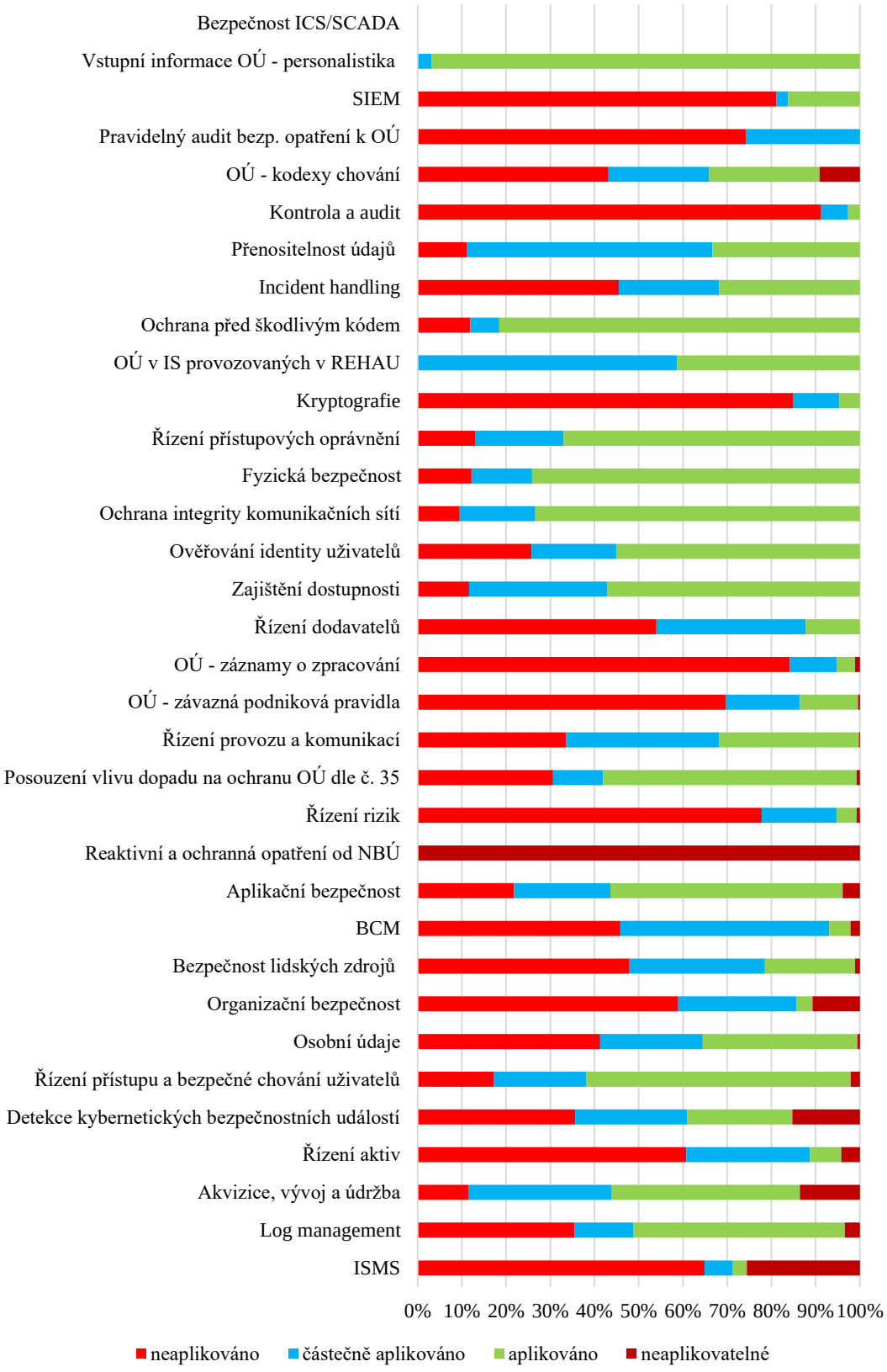
Druhý graf (Graf 26.) obsahuje také četnosti hodnocení jednotlivých povinností, ale jsou zde vynechány nerelevantní povinnosti. Vidíme, že nejvíce aplikovaných povinností je v oblasti Vstupní informace OÚ - personalistika, dále v Ochraně před škodlivým kódem, ve Fyzické bezpečnosti, Ochraně integrity komunikačních sítí a Řízení přístupových oprávnění. Tyto oblasti jsou společnostmi ve velké míře dobře podchycené. V oblasti Vstupní informace OÚ - personalistika dokonce nejsou žádná neaplikovaná ani neaplikovatelné povinnosti. Druhý extrém můžeme vidět v oblasti Reaktivní a ochranná opatření od NBÚ. Zde jsou pouze neaplikovatelné povinnosti.

Největší problém mají společnosti s oblastmi: Kontrola a audit, Kryptografie, OÚ - záznamy o zpracování, Řízení rizik a SIEM. V těchto oblastech je většina povinností neaplikovaných. Hodnoty se pohybují okolo 84 %, v případě kontroly a auditu je to více než 90 %.

Nejmenší počty neaplikovaných řešení jsou v oblastech: Ochrana integrity komunikačních sítí, Přenositelnost údajů, Ochrana před škodlivým kódem, Řízení přístupových oprávnění, Fyzická bezpečnost, Zajištění dostupnosti a Akvizice, vývoj a údržba. V těchto oblastech je zhruba 12 % řešení neaplikovaných.



Graf 25: Hodnocení řešení v jednotlivých oblastech.[Zdroj: vlastní zpracování]



Graf 26: Hodnocení relevantních řešení v jednotlivých oblastech.[Zdroj: vlastní zpracování]

Celkově můžeme říci, že oblasti Fyzická bezpečnost, Ochrana integrity komunikačních sítí, Řízení přístupových oprávnění, Ochrana před škodlivým kódem nebo Vstupní informace OÚ – personalistika, jsou velmi dobře zvládnuté ve všech společnostech.

V další části se zaměříme na konkrétní povinnosti a jejich hodnocení. Zobrazíme si u každého typu hodnocení žebříček deseti povinností, které mají nejvyšší počet daných hodnocení. Tedy jsou aplikovány / neaplikovány / nerelevantní / neaplikovatelné / částečně aplikovány u největšího počtu sledovaných společností.

Nerelevantní

Nerelevantní hodnocení je celkem u 30 % otázek. Které konkrétní povinnosti jsou tedy pro testované společnosti zbytečné? Následující tabulka (Tabulka č. 3) popisuje deset povinností, které jsou pro největší počet společností nerelevantní. Zde najdeme několik povinností, které jsou nerelevantní pro všechny sledované společnosti.

Tabulka 3: Povinnosti s nejvyšším výskytem nerelevantních hodnot.[Zdroj: vlastní zpracování]

Oblast	Povinnost	Nerele-vantní	%
Bezpečnost ICS/SCADA	Zajištěno omezení fyzického přístupu k síti a zařízením průmyslových a řídících systémů.	34	100 %
Bezpečnost ICS/SCADA	Zajištěno omezení propojení a vzdáleného přístupu k síti průmyslových a řídících systémů.	34	100 %
Bezpečnost ICS/SCADA	Zajištěna ochrana jednotlivých technických aktiv průmyslových a řídících systémů před využitím známých zranitelností.	34	100 %
Bezpečnost ICS/SCADA	Zajištěno obnovení chodu průmyslových a řídících systémů po kybernetickém bezpečnostním incidentu.	34	100 %
OÚ - kodexy chování	Vydáno osvědčení podle čl. 40 GDPR.	33	97 %
Incident handling	Povinnost hlásit kybernetické bezpečnostní incidenty, a to bezodkladně po jejich detekci Národnímu bezpečnostnímu úřadu (Vládnímu CERT týmu).	31	91 %

BCM	Jsou stanoveny a aktualizovány postupy pro provedení opatření vydaných NBÚ podle § 13 a 14 ZKB, ve kterých jsou zohledněny: Stav dotčených bezpečnostních opatření.	31	91 %
Reaktivní a ochranná opatření od NBÚ	Jsou řešena reaktivní opatření vydaná NBÚ.	31	91 %
Organizační bezpečnost	Zavedena organizace řízení bezpečnosti informací (organizační bezpečnost), v rámci, které je určen výbor pro řízení kybernetické bezpečnosti a bezpečnostní role a jejich práva a povinnosti související s ICT.	30	88 %
Organizační bezpečnost	Určena bezpečnostní role: architekt kybernetické bezpečnosti.	29	85 %

U všech společností se považuje za nerelevantní zavádět povinnosti z oblasti Bezpečnost ICS/SCADA. Což je oblast zahrnující bezpečnost průmyslových řídících systémů a SCADA systémů.

Neaplikováno

Zaměříme se nyní na oblast neaplikovaných povinností. Tabulka (Tabulka 4.) obsahuje deset povinností, které společnosti nejčastěji neaplikují. Nalezneme zde několik povinností z oblasti Kontroly a auditu, Bezpečnosti lidských zdrojů, Kryptografie nebo z Osobních údajů. Tyto oblasti tedy obsahují povinnosti, které neaplikuje největší počet sledovaných firem.

Tabulka 4: Nejčastěji neaplikované povinnosti.[Zdroj: vlastní zpracování]

Oblast	**Povinnost**	**neapli-kováno**	**%**
Kontrola a audit	V rámci pravidelné kontroly a auditu je posouzen soulad bezpečnostních opatření s obecně závaznými právními předpisy, vnitřními předpisy, jinými předpisy a smluvními	32	94 %

	závazky vztahujícími se ke kybernetické bezpečnosti a jsou určena opatření pro jeho prosazování.		
Bezpečnost lidských zdrojů	Je hodnocena účinnost plánu rozvoje bezpečnostního povědomí, provedených školení a dalších činností spojených s prohlubováním bezpečnostního povědomí.	30	88 %
Kontrola a audit	V rámci pravidelné kontroly a auditu jsou prováděny a dokumentovány pravidelné kontroly dodržování bezpečnostní politiky a výsledky těchto kontrol jsou zohledněny v plánu rozvoje bezpečnostního povědomí a plánu zvládání rizik.	30	88 %
Bezpečnost lidských zdrojů	Je stanoven plán rozvoje bezpečnostního povědomí, který obsahuje formu, obsah a rozsah potřebných školení a jsou určeny osoby provádějící realizaci jednotlivých činností, které jsou v plánu uvedeny.	30	88 %
Kryptografie	Bezpečnostní politika: Používání kryptografické ochrany.	30	88 %
Bezpečnost lidských zdrojů	Jsou určena pravidla a postupy pro řešení případů porušení stanovených bezpečnostních pravidel ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role (disciplinární řízení).	29	85 %
Řízení provozu a komunikací	S ohledem na klasifikaci aktiv je prováděna výměna a předávání informací na základě písemných smluv, jejichž součástí je ustanovení o bezpečnosti informací.	27	79 %
Osobní údaje	Role příjemce dat (popis?)	27	79 %
Kryptografie	Pro používání kryptografické ochrany je stanovena úroveň ochrany s ohledem na typ a sílu kryptografického algoritmu.	27	79 %
Osobní údaje	Plánujete zavést pravidelná školení pro práci s osobními daty?	27	79 %

Celých 32 vzorků má problém s aplikováním kontroly a auditu, při kterém se posoudí soulad bezpečnostních opatření s různými předpisy a závazky vztahující se ke kybernetické bezpečnosti a také s určením opatření, které je budou prosazovat. Aby tato povinnost byla aplikována, musí být v bezpečnostní politice uvedeny veškeré předpisy a závazky (obecně závazné právní, vnitřní a jiné předpisy, smluvní závazky), které se vztahují k systému. Souladem se myslí nenarušení soukromí zaměstnanců nebo

neohrožení jejich bezpečnosti, nenarušení obchodního tajemství nebo že existuje soulad opatření se smlouvami s dodavateli. Hodnotí se také, zda dbají na promítnutí zákonů nebo vyhlášek do ISMS. Je třeba řešit, zda a jak počítají s úpravami smluv, předpisů a jak je zapracovávají do směrnic. Aby tato povinnost byla uznána za aplikovanou, musí společnost podávat zprávu z auditu, vyhodnocovat jej a měly by existovat doporučení pro auditora.

Velká většina vzorků také neaplikuje hodnocení účinnosti plánu rozvoje bezpečnostního povědomí, provedených školení a dalších činností spojených s prohlubováním bezpečnostního povědomí. Pověřená osoba u této povinnosti zjišťuje, zda je účinnost hodnocena, jakou formou, kde je to uloženo a v jakém časovém intervalu se hodnocení provádí. Musí být stanoveny metriky pro měření účinnosti a na základě zjištění by měly být určeny a provedeny opatření, pak by tato povinnost byla považována za aplikovanou. Stejný počet vzorků neaplikuje v rámci pravidelné kontroly a auditu provádění a dokumentaci pravidelných kontrol dodržování bezpečnostní politiky a zohlednění výsledků těchto kontrol v plánu rozvoje bezpečnostního povědomí a plánu zvládání rizik. Aby byla povinnost aplikována, musí společnosti mít nastavená pravidla a postupy pro přezkoumání systému řízení bezpečnosti, musí se vytvářet zprávy z přezkoumání systému řízení bezpečnosti informací. Kontrolují se plány rozvoje bezpečnostních povědomí, plány zvládání rizik. Měla by se evidovat pravidelná školení zaměstnanců, jejich vyhodnocování. Dále se hlídá, zda se kontrolují události a incidenty, které jsou způsobeny zaměstnanci a zda na to společnost reaguje změnou školení, upravením hrozeb apod.

Další tabulka (Tabulka č. 5) ukazuje povinnosti, které mají nejmenší počet hodnocení neaplikováno. Tyto povinnosti jsou ve většině případů převážně nerelevantní.

Tabulka 5: Nejméně často neaplikované povinnosti.[Zdroj: vlastní zpracování]

Oblast	**Povinnost**	**neapli-kováno**
Bezpečnost ICS/SCADA	Zajištěno omezení fyzického přístupu k síti a zařízením průmyslových a řídících systémů.	0

Bezpečnost ICS/SCADA	Zajištěno omezení propojení a vzdáleného přístupu k síti průmyslových a řídících systémů.	0
Bezpečnost ICS/SCADA	Zajištěna ochrana jednotlivých technických aktiv průmyslových a řídících systémů před využitím známých zranitelností.	0
Bezpečnost ICS/SCADA	Zajištěno obnovení chodu průmyslových a řídících systémů po kybernetickém bezpečnostním incidentu.	0
BCM	Jsou stanoveny a aktualizovány postupy pro provedení opatření vydaných NBÚ podle § 13 a 14 ZKB, ve kterých jsou zohledněny: Stav dotčených bezpečnostních opatření.	0
Reaktivní a ochranná opatření od NBÚ	Jsou řešena reaktivní opatření vydaná NBÚ.	0
Akvizice, vývoj a údržba	Je zajištěna bezpečnost vývojového prostředí a zároveň je zajištěna ochrana používaných testovacích dat.	0
Aplikační bezpečnost	Je zajištěna trvalá ochrana aplikací a informací dostupných z vnější sítě před neoprávněnou činností, popřením provedených činností, kompromitací nebo neautorizovanou změnou.	0
Osobní údaje	Jsou osobní údaje v databázi zákazníků? Pokud jsou Vaše vykonáváte správu dle smluvních ujednání?	0
Posouzení vlivu dopadu na ochranu osobních údajů dle č. 35	Zpracováváte data o zaměstnancích, zdravotně postižených nebo o nezletilých?	0
OÚ v IS provozovaných v REHAU	V jakých IS jsou data bezpečně zpracovávána, uchovávána? Jsou ve Vámi vlastněných a využívaných IS data bezpečně zpracovávána, uchovávána?	0
Ochrana integrity komunikačních sítí	Pro ochranu integrity rozhraní vnější komunikační sítě je zavedeno: Jsou využívány nástroje pro ochranu integrity vnitřní komunikační sítě, které zajistí její segmentaci.	0
Řízení provozu a komunikací	Je prováděno pravidelné zálohování a prověřování použitelnosti provedených záloh.	0

Vstupní informace OÚ - personalistika	Máte kompletní přijímací dokumentaci zpracovanou?	0
Řízení provozu a komunikací	Bezpečnostní politika: Poskytování a nabývání licencí programového vybavení a informací.	0
Zajištění dostupnosti	Zálohování důležitých technických aktiv je řešeno využitím redundance v návrhu řešení.	0
Ochrana integrity komunikačních sítí	Pro ochranu integrity rozhraní vnější komunikační sítě je zavedeno: Řízení bezpečného přístupu mezi vnější a vnitřní sítí	0
Osobní údaje	Při zpracování osobních údajů je zajištěna schopnost obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů.	0

Částečně aplikováno

Částečně aplikovaných řešení nebo povinností je 16 %. Které povinnosti jsou nejčastěji pouze částečně aplikované je vidět z tabulky (Tabulka 6.) níže. Je zde více povinností z oblastí Bezpečnosti lidských zdrojů, Osobních údajů nebo Řízení dodavatelů.

Tabulka 6: Nejvíce částečně aplikované povinnosti.[Zdroj: vlastní zpracování]

Oblast	**Povinnost**	**částečně apliko-váno**	**%**
Bezpečnost lidských zdrojů	Jsou stanovena pravidla pro určení osob, které budou zastávat bezpečnostní role, role administrátorů nebo uživatelů.	24	71 %
Bezpečnost lidských zdrojů	Bezpečnostní politika: Bezpečné chování uživatelů.	23	68 %

Osobní údaje	S přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, provedou správce a zpracovatel vhodná technická a organizační opatření, aby zajistili úroveň zabezpečení odpovídající danému riziku (opatření dle GDPR v závislosti na rizicích).	22	65 %
Osobní údaje	Garantují Vaši dodavatelé bezpečnost zpracovávaných osobních údajů?	22	65 %
BCM	Jsou stanoveny cíle BCM formou určení: Doby obnovení chodu, během které bude po kybernetickém bezpečnostním incidentu obnovena minimální úroveň poskytovaných klíčových služeb (závislých na ICT) (RTO).	20	59 %
Řízení provozu a komunikací	Bezpečnostní politika: Zálohování a obnova.	20	59 %
Řízení dodavatelů	S dodavateli se uzavírá dohoda o úrovni poskytovaných služeb (SLA), která stanoví způsoby a úrovně realizace bezpečnostních opatření a určí vztah vzájemné smluvní odpovědnosti za zavedení a kontrolu bezpečnostních opatření.	19	56 %
Řízení provozu a komunikací	Výměna a předávání informací je prováděna na základě pravidel stanovených právními předpisy za současného zajištění bezpečnosti informací a tato pravidla jsou dokumentována.	18	53 %
Řízení dodavatelů	Jsou stanovena pravidla pro dodavatele, která zohledňují potřeby řízení bezpečnosti informací, a řídí své dodavatele nebo jiné externí subjekty, které se podílejí na rozvoji, provozu nebo zajištění bezpečnosti ICT.	17	50 %
OÚ - závazná podniková pravidla	V rámci zpracovávání OÚ jsou stanovena závazná podniková pravidla vymezující použití obecných zásad pro ochranu údajů, zejména účelové omezení, minimalizaci údajů, omezenou dobu uložení, kvalitu údajů, záměrná a standardní ochranu osobních údajů, právní základ pro zpracování, zpracování zvláštních kategorií osobních údajů; opatření k zajištění zabezpečení údajů a požadavky ohledně dalšího	17	50 %

	předávání subjektům, které podnikovými pravidly nejsou vázány.		

Ze sledovaných 34 vzorků celkem 24 aplikuje pouze částečně povinnost stanovení pravidel pro určení osob, které budou zastávat bezpečnostní role, role administrátorů nebo uživatelů. Kontroluje se, zda jsou tato pravidla stanovena, kde je najdeme, v jaké jsou formě a kdo je kontroluje. Pravidla by měla odpovídat realitě, což se hodnotí ze záznamů o vykonávání funkcí, zda tyto skutečnosti odpovídají pravidlům.

Celkem 68 % společností aplikuje pouze částečně bezpečnostní politiku, konkrétně bezpečné chování uživatelů. To znamená, že mají částečně vytvořenou politiku zaměřenou na bezpečnost uživatelů a na jejich bezpečné chování. U této povinnosti se kontroluje i bezpečnost lidských zdrojů a řízení přístupu a bezpečné chování uživatelů. Měla by být určena pravidla pro bezpečné nakládání s aktivy, bezpečné zacházení s hesly nebo bezpečné použití elektronické pošty. Dále jde o bezpečné chování na internetu, sociálních sítích, bezpečný vzdálený přístup, bezpečnost ve vztahu k mobilním zařízením.

Aplikováno

Podíváme se také na povinnosti, které společnostem obvykle nepůsobí problémy. Tabulka (Tabulka 7.) obsahuje deset povinností, které jsou ve společnostech nejčastěji aplikované. Společnosti často aplikují povinnosti z oblastí Ochrany před škodlivým kódem, Osobních údajů nebo Řízení přístupu či přístupových oprávnění. Nenašli jsme však ani jednu povinnost, kterou by mělo aplikováno všech 34 sledovaných vzorků.

Tabulka 7: Nejčastěji aplikované povinnosti.[Zdroj: vlastní zpracování]

Oblast	**Povinnost**	**aplikováno**	**%**
Ochrana před škodlivým kódem	Jsou prováděny pravidelné aktualizace nástrojů pro ochranu před škodlivým kódem, jejich definic a signatur.	33	97 %

Řízení přístupových oprávnění	Je používán nástroj pro řízení přístupových oprávnění, kterým zajišťuje řízení oprávnění: Pro přístup k jednotlivým aplikacím a datům.	31	91 %
Řízení přístupu a bezpečné chování uživatelů	Přistupujícím aplikacím je přidělen samostatný identifikátor.	31	91 %
Ochrana před škodlivým kódem	Je používán nástroj pro ochranu před škodlivým kódem, který zajistí ověření a stálou kontrolu: Komunikace mezi vnitřní sítí a vnější sítí.	31	91 %
Vstupní informace OÚ - personalistika	Máte kompletní přijímací dokumentaci zpracovanou?	31	91 %
Osobní údaje	Disponujete "papírovými osobními údaji"? Přistupujete k osobním údajů v nestrojové podobě jako k těm strojovým?	31	91 %
Osobní údaje	Při zpracování osobních údajů je zajištěna schopnost obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů.	30	88 %
Zajištění dostupnosti	Zálohování důležitých technických aktiv je řešeno využitím redundance v návrhu řešení.	29	85 %
Řízení přístupu a bezpečné chování uživatelů	Každému uživateli je přiřazen jednoznačný identifikátor (každý uživatel má své vlastní autentizační údaje).	29	85 %
Řízení přístupu a bezpečné chování uživatelů	Je omezeno přidělování administrátorských oprávnění.	29	85 %

Kromě jedné sledované společnosti všechny aplikují provádění pravidelné aktualizace nástrojů pro ochranu před škodlivým kódem, jejich definic a signatur. To znamená, že tyto společnosti mají jasně definovaná pravidla pro aktualizaci antiviru, mají popsána pravidla pro jednotlivé případy v oblasti ochrany před škodlivým kódem. Tyto aktualizace musí být definovány v politikách a měly by být v souladu se záznamy v databázích. Kontroluje se tedy poslední aktualizace jádra, databáze antiviru, stanic nebo serverů.

Další často aplikovanou povinností, celkem 31 ze 34 vzorků ji má aplikovánu, je nástroj pro řízení přístupových oprávnění pro přístup k jednotlivým aplikacím a datům. To znamená, že společnosti mají nastavena oprávnění uživatelů, tedy roli na úrovni aplikace a operačního systému a mají nastaven firewall pro řízení přístupu na základě IP adres.

Neaplikovatelné

Neaplikovatelných povinností je pouze 1 %. Které konkrétní povinnosti jsou nejčastěji neaplikovatelná vidíme níže (Tabulka 8.). V získaných asistovaných zhodnoceních není ani jedna povinnost, která by byla neaplikovatelná u velkého počtu vzorků.

Tabulka 8: Nejvíce neaplikovatelné povinnosti.[Zdroj: vlastní zpracování]

Oblast	Povinnost	neapli-kova-telné	%
Log management	Pomocí nástroje pro zaznamenávání činnosti informačního/komunikačního systému je zaznamenáváno(y): Přístupy k záznamům o činnostech, pokusy o manipulaci se záznamy o činnostech a změny nastavení nástroje pro zaznamenávání činností.	5	15 %
Akvizice, vývoj a údržba	Je zajištěna bezpečnost vývojového prostředí a zároveň je zajištěna ochrana používaných testovacích dat.	4	12 %

Řízení přístupu a bezpečné chování uživatelů	Přidělování a odebírání přístupových oprávnění je prováděno v souladu s politikou řízení přístupu.	4	12 %
Akvizice, vývoj a údržba	Jsou stanoveny bezpečnostní požadavky na změny ICT spojené s jejich akvizicí, vývojem a údržbou a jsou zahrnuty do projektu akvizice, vývoje a údržby systému.	4	12 %
Akvizice, vývoj a údržba	Jsou identifikovány, hodnoceny a řízeny rizika související s akvizicí, vývojem a údržbou systémů.	4	12 %
Detekce kybernetických bezpečnostních událostí	Je používán nástroj pro detekci kybernetických bezpečnostních událostí, který vychází ze stanovených bezpečnostních potřeb a výsledků hodnocení rizik a který zajistí ověření, kontrolu a případné zablokování komunikace mezi vnitřní komunikační sítí a vnější sítí.	4	12 %
ISMS	Stanovena bezpečnostní politika ISMS	4	12 %
ISMS	Stanoven rozsah a hranice ISMS. (Je určeno, kterých organizačních částí a technických prvků se ISMS týká.)	4	12 %
ISMS	Je prováděna aktualizace ISMS a související dokumentace na základě zjištění auditů/penetračních testů, výsledků hodnocení účinnosti ISMS a v souvislosti s prováděnými změnami.	4	12 %
Řízení aktiv	Určena bezpečnostní role: garant/vlastník aktiva.	4	12 %

Nejvíce neaplikovatelnou povinností, kterou nemůže aplikovat 5 ze sledovaných firem, je zaznamenávání činnosti informačního nebo komunikačního systému pomocí nástroje. Tento nástroj by měl zaznamenávat přístup k záznamům o činnostech, pokusy o manipulaci se záznamy o činnostech a změny nastavení tohoto nástroje.

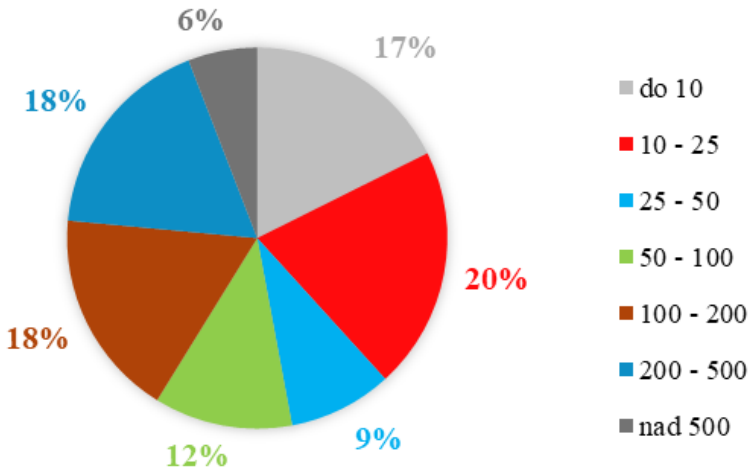
4.4 Pohled na data dle velikosti vzorků

Získané vzorky byly rozděleny do 7 skupin podle počtu zaměstnanců. Níže je popsáno (Tabulka č. 9) které vzorky se vyskytují ve které skupině. Dále tabulka ukazuje intervaly počtů zaměstnanců jednotlivých skupin.

Tabulka 9: Počty a čísla vzorků dle počtu zaměstnanců.[Zdroj: vlastní zpracování]

Čísla vzorků	Počet vzorků	Počet zaměstnanců
3, 4, 20, 26, 31, 34	6	do 10
11, 16, 19, 22, 27, 28, 30	7	10–25
8, 10, 32	3	25–50
5, 21, 24, 33	4	50–100
1, 7, 9, 12, 14, 29	6	100–200
13, 15, 17, 18, 23, 25	6	200–500
6, 2	2	nad 500

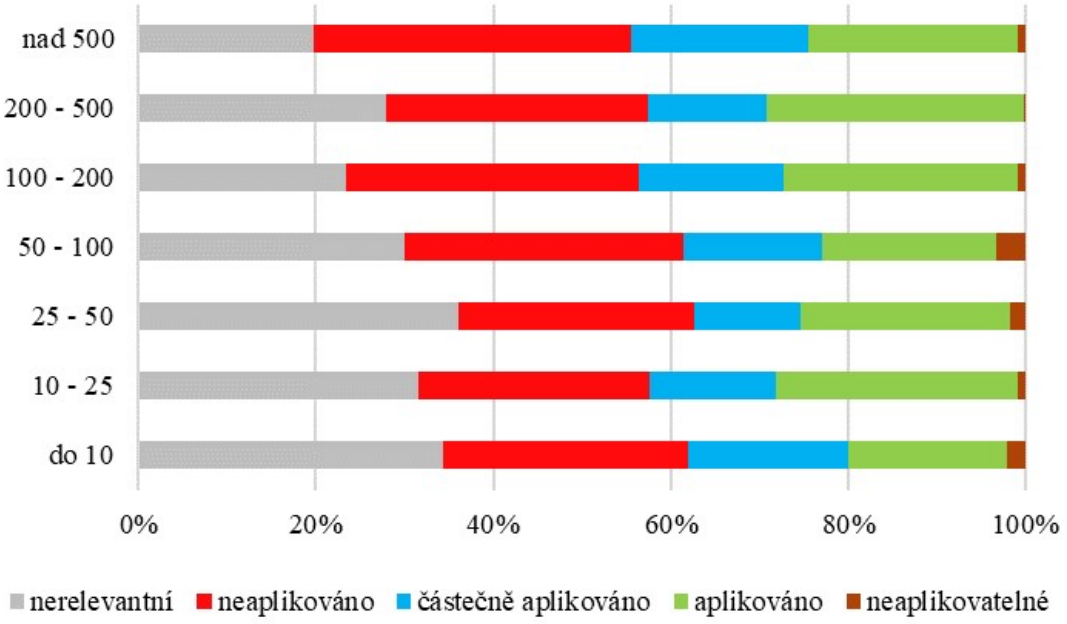
Počty vzorků v jednotlivých skupinách ukazuje i koláčový graf (Graf č. 27). Popisuje procentuální podíl vzorků ve skupinách dle počtu zaměstnanců. Jak můžeme vidět, nejvíce testovaných společností je ve skupině malých firem s počtem zaměstnanců 10–25. Dále je zde velké zastoupení velkých firem s počtem 100–200 a 200–500 zaměstnanců.



Graf 27: Počty vzorků ve skupinách dle počtu zaměstnanců.[Zdroj: vlastní zpracování]

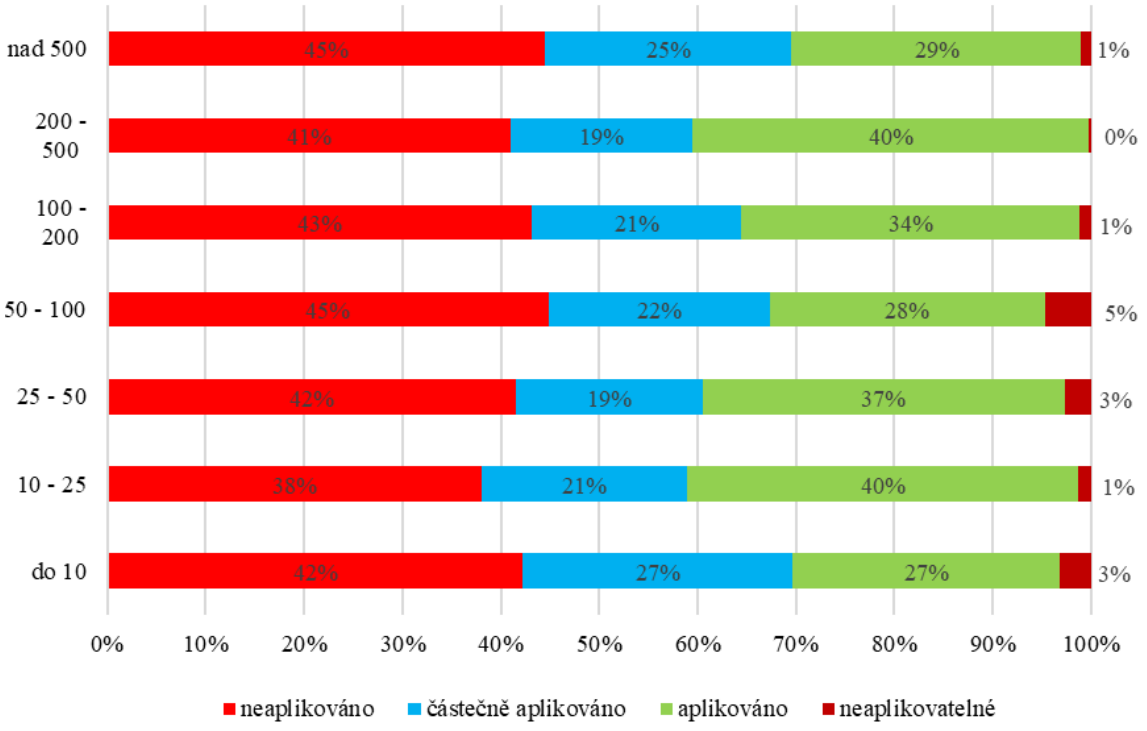
Nyní se podíváme, jaká jsou hodnocení povinností v jednotlivých skupinách (Graf č. 28). Můžeme si všimnout, že s rostoucím počtem zaměstnanců klesá počet nerelevantních řešení. Tento trend je logický, větší společnosti musí aplikovat větší množství

povinností.



Graf 28: Srovnání hodnocení dle počtu zaměstnanců.[Zdroj: vlastní zpracování]

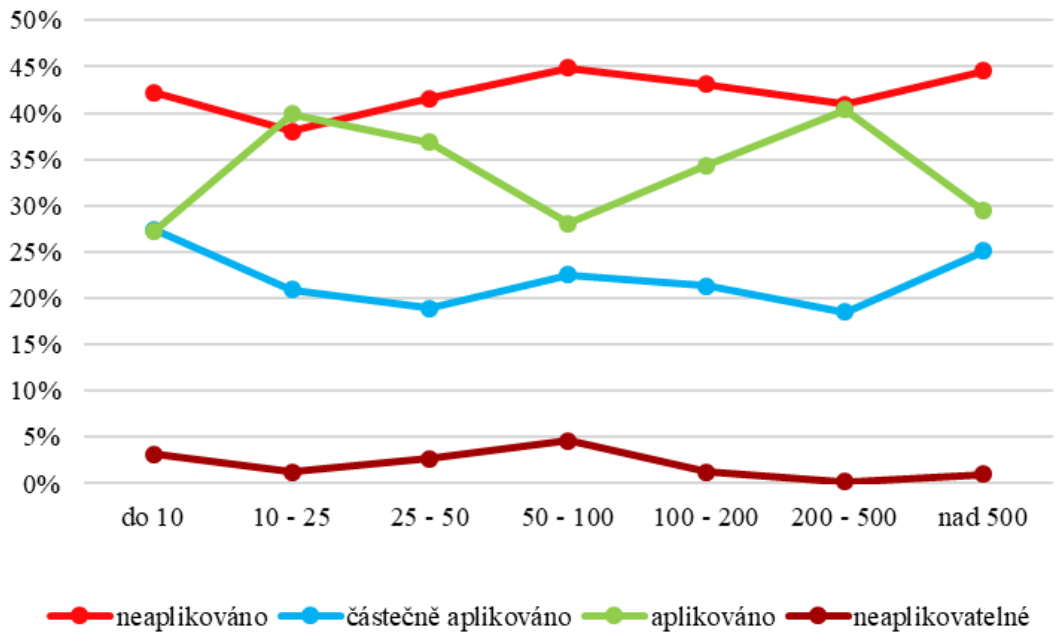
Pro lepší přehlednost a porovnávání si zobrazíme graf bez nerelevantních povinností (Graf č. 29).



Graf 29: Srovnání hodnocení dle počtu zaměstnanců (relevantní).[Zdroj: vlastní zpracování]

Jak můžeme vidět, nejlépe jsou na tom vzorky ve skupině 200–500 a 10–25 zaměstnanců. V těchto dvou skupinách je největší podíl aplikovaných povinností, nejmenší podíl neaplikovaných řešení a minimum neaplikovatelných povinností. Nejhůře dopadla skupina 50–100. V této skupině je největší podíl neaplikovaných řešení, nízké procento aplikovaných povinností a velký podíl neaplikovatelných řešení.

V těchto grafech existuje jakýsi trend, proto jsou hodnocení různých povinností vykresleny ještě i ve spojnicovém grafu (Graf 30.). Můžeme si všimnout, že mikro podniky (do 10 zaměstnanců), střední podniky (50–100 zaměstnanců) a velké podniky (nad 500 zaměstnanců) jsou na tom velice podobně, hůře než ostatní. Tyto společnosti vykazují vysoký podíl neaplikovaných povinností i neaplikovatelných. Aplikovaných řešení u těchto společností je malý podíl. Naopak podniky, jejichž velikost se nachází mezi výše zmíněnými jsou na tom mnohem lépe. Byl tedy nalezen kolísavý trend v závislosti na velikosti společnosti.



Graf 30: Spojnicový graf hodnocení povinností dle velikosti.[Zdroj: vlastní zpracování]

Dále byla analýza zaměřena na hledání shluků v jednotlivých oblastech. Tedy šlo nám o zjištění, zda společnosti vykazují stejná hodnocení povinností v některých oblastech.

Mikro podniky (do 10 zaměstnanců) mají obvykle řešenou Fyzickou bezpečnost a Ochranu před škodlivým kódem. Neaplikují však Závazná podniková pravidla v oblasti Osobních údajů a nevedou Záznamy o zpracování osobních údajů. Pro tyto mikro společnosti jsou nerelevantní oblasti: Bezpečnost ICS/SCADA, SIEM, Incident handling, Posouzení vlivu dopadu na ochranu osobních údajů dle č. 35.

Drobné společnosti (10–25 zaměstnanců) aplikují stejně jako mikro podniky Fyzickou bezpečnost, Ochranu před škodlivým kódem, ale navíc i Ochranu integrity komunikačních sítí, řeší Log management a Dostupnost. Nerelevantních je pro tuto velikost firem větší počet oblastí: ISMS, Řízení rizik, Organizační bezpečnost, Bezpečnost ICS/SCADA, Detekce kybernetických bezpečnostních událostí, SIEM a Incident handling. Tyto podniky však vůbec neaplikují Kryptografii, nevedou Záznamy o zpracování osobních údajů, nevytváří Kategorizace osobních údajů a nezavádí pravidelná školení pro práci s osobními daty. Ve velké míře mají tedy problém s Osobními údaji.

Menší společnosti (25–50 zaměstnanců) zcela aplikují Fyzickou bezpečnost a z velké části Ochranu integrity komunikačních sítí, Řízení přístupových oprávnění a Akvizici, vývoj a údržbu. Nerelevantní jsou pro ně oblasti: ISMS, Organizační bezpečnost, Bezpečnost ICS/SCADA, Detekce kybernetických bezpečnostních událostí, SIEM, Incident handling a BCM. Tyto společnosti však zcela neprovádí kontroly a audity a neřeší role správce, příjemce a zpracovatele osobních údajů.

Střední podniky (50–100 zaměstnanců) vykazují nejméně shluků, většinou jsou hodnocení povinností zcela různé. Z velké části však všechny tyto společnosti aplikují Log management, Fyzickou bezpečnost, Ochranu integrity komunikačních sítí a Ochranu před škodlivým kódem. Neřeší však Kryptografii, neprovádí Kontroly ani audity, neaplikují Kodexy chování ani Závazná podniková pravidla v oblasti osobních údajů. Nerelevantní pro ně jsou oblasti: Bezpečnost ICS/SCADA, SIEM, Incident handling a BCM.

Společnosti s počtem zaměstnanců 100–200 stejně jako předchozí vykazují menší počty shluků a hodnocení jsou spíše různorodá napříč společnostmi. Z velké části neaplikují Řízení rizik ani aktiv. Aplikují však Ochranu před škodlivým kódem a Ochranu integrity komunikačních sítí. Z velké části se snaží aplikovat Řízení přístupu a bezpečné chování uživatelů. Nerelevantní jsou pro ně oblasti: Bezpečnost ICS/SCADA, SIEM, In-

cident handling.

Větší společnosti (200–500 zaměstnanců) aplikují Fyzickou bezpečnost, Ochranu integrity komunikačních sítí a Povinnosti ochrany před škodlivým kódem. Z velké části aplikují také Řízení přístupu, Ověřování identity uživatelů, Řízení přístupových oprávnění a Akvizici, vývoj a údržbu. Na druhou stranu tyto velké společnosti neřeší Řízení aktiv a z velké části ani Řízení rizik. Ani jedna ze společností nemá aplikovány povinnosti z oblasti Kryptografie, dále neaplikují SIEM ani Incident handling. Nerelevantní jsou pro ně oblasti: Organizační bezpečnost, Bezpečnost ICS/SCADA.

Velké podniky (nad 500 zaměstnanců) mají dobře podchycenou oblast Řízení přístupu a bezpečného chování uživatelů. Aplikovány mají také povinnosti Fyzické bezpečnosti a Ochrany před škodlivým kódem. Neaplikují však Řízení rizik, což se u takto velkých firem nepředpokládá, spíše naopak. Neprovádí Kontrolu ani audity a mají velké potíže s povinnostmi týkajícími se Osobních údajů. Nerelevantní je pro ně pouze oblast Bezpečnost ICS/SCADA.

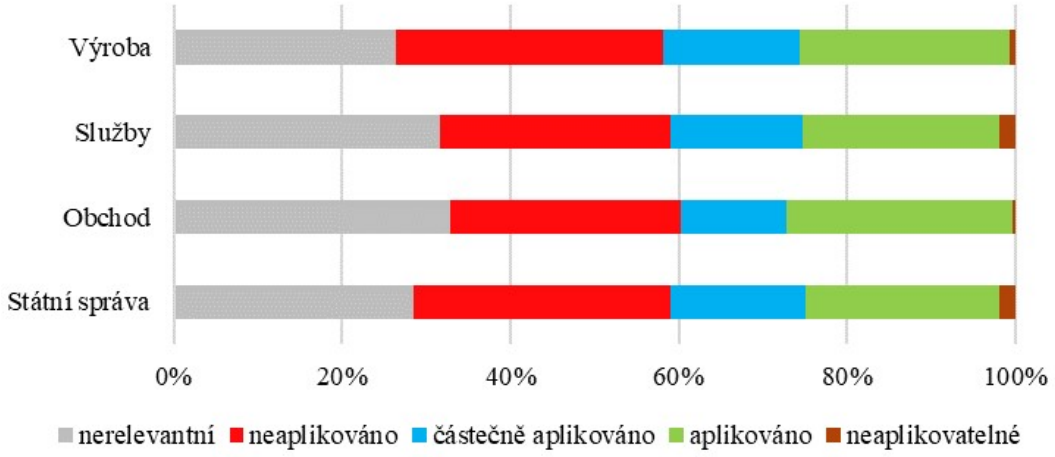
4.5 Pohled na data dle oborů podnikání

Nyní budeme získaná data analyzovat z pohledu oboru podnikání. Společnosti jsou rozděleny do 4 oborů: státní správa, obchod, služby a výroba. Konkrétní rozdělení můžeme vidět v tabulce (Tabulka č. 10) níže.

Tabulka 10: Počty vzorků dle oboru podnikání.[Zdroj: vlastní zpracování]

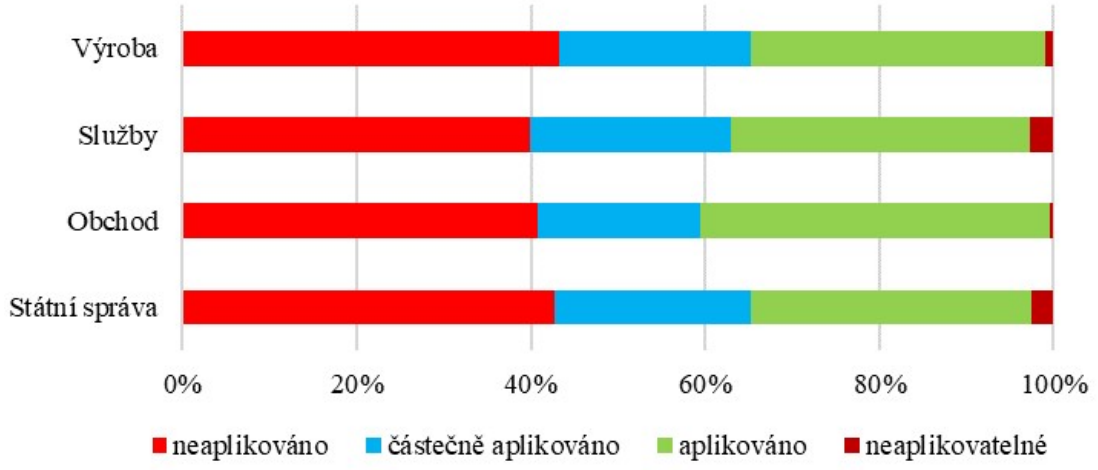
Obor	Počet vzorků	Číslo vzorku
Státní správa	8	4, 17, 21, 22, 24, 29, 30, 33
Obchod	5	10, 15, 16, 26, 32
Služby	11	3, 5, 7, 8, 9, 18, 19, 20, 23, 27, 34
Výroba	10	1, 2, 6, 11, 12, 13, 14, 25, 28, 31

Následující graf (Graf č. 31) zobrazuje hodnocení povinností dle oboru podnikání. Na první pohled můžeme vidět, že v oboru výroby a ve státní správě je menší počet nerelevantních povinností. Naopak v oblasti služeb a obchodu jich je více než 30 %.



Graf 31: Hodnocení povinností dle oboru podnikání.[Zdroj: vlastní zpracování]

Pro vhodnější porovnání zobrazíme graf bez nerelevantních řešení (Graf 32.). Ve výrobě a státní správě je 43 % neaplikovaných povinností. V oblasti obchodu jich je 41 % a ve službách 40 %. Aplikovaných povinností nalezneme nejvíce v obchodě, zde je to celkem 40 %. Dále je 34 % aplikovaných povinností ve službách a výrobě a 32 % ve státní správě. Ve službách je 2,8 % neaplikovatelných povinností, o něco méně jich je ve státní správě, 2,6 %. Ve výrobě nalezneme 1 % neaplikovatelných povinností a nejméně jich je v obchodě, pouhých 0,5 %.



Graf 32: Hodnocení relevantních povinností dle oboru podnikání.[Zdroj: vlastní zpracování]

Jak se zdá, nejlépe jsou na tom společnosti podnikající v oblasti obchodu. Ty vykazují nejvyšší počet aplikovaných povinností a nižší počet neaplikovaných řešení. V tomto

oboru je také nejméně neaplikovatelných a částečně aplikovaných povinností.

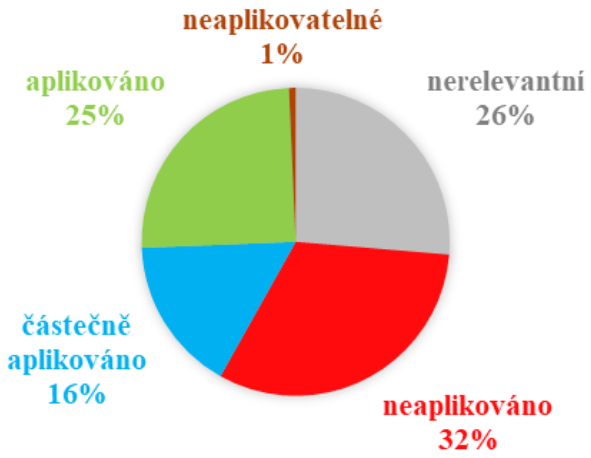
Nyní se podíváme na to, které oblasti jsou v oborech problémové a které naopak ne. Tedy nejčastěji neaplikované, aplikované a neaplikovatelné.

Výroba

Ve výrobě je 73 % povinností z oblasti Kontroly a auditu a také z oblasti Osobních údajů - záznamy o zpracování neaplikovaných. Dále výrobní podniky neaplikují 60 % povinností z oblastí Kryptografie a Pravidelného auditu bezpečnostních opatření k osobním údajům. Polovinu povinností neaplikují také v oblasti Řízení rizik, Řízení dodavatelů nebo Řízení aktiv.

Ve výrobě aplikují veškeré povinnosti z oblasti Vstupních informací osobních údajů - personalistika. Dále aplikují 88 % povinností z Ochrany před škodlivým kódem, 80 % z oblasti Fyzické bezpečnosti. Povinnosti z oblastí Zajištění dostupnosti a Ochrany integrity komunikačních sítí aplikují jen 68 %. Oblast Řízení přístupových oprávnění a Řízení přístupu a bezpečné chování uživatelů aplikují již zhruba ze 60 %.

Celkem 10 % povinností nelze aplikovat v oblastech Akvizice, vývoje a údržby a Reaktivních a ochranných opatření od NBÚ. Něco málo přes 4 % povinností je ve výrobě neaplikovatelných z oblasti Log managementu. Další oblasti jsou neaplikovatelné méně než ze 2 %.



Graf 33: Hodnocení povinností ve výrobě.[Zdroj: vlastní zpracování]

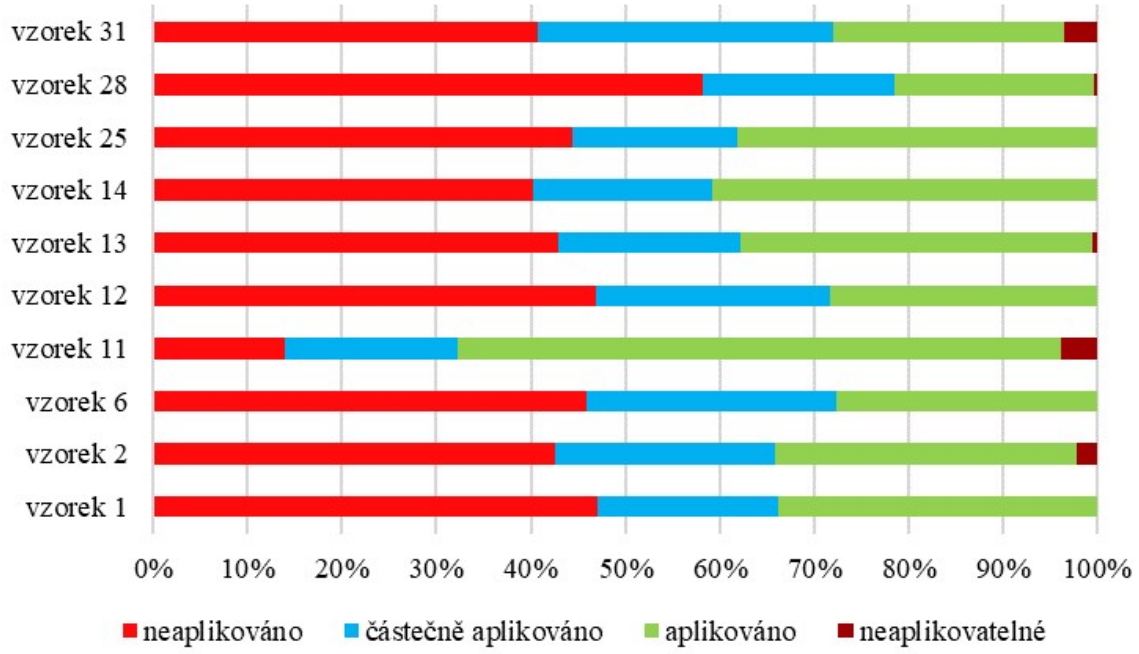
Průměrným hodnocením ve výrobě je hodnocení neaplikováno, stejně tak je to nejčastějším hodnocením.

Podíváme se také na konkrétní povinnosti, které mají nejvyšší počty jednotlivých hodnocení. Všechny výrobní společnosti neřeší smluvně dodavatelský řetězec ani bezpečnost jejich dat u dodavatelů. Jelikož jde o výrobní podniky, které obvykle spolupracují s větším počtem dodavatelů než v jiných oborech, je zarážející, že není aplikována ani u jedné ze sledovaných výrobních firem.

Z 10 sledovaných výrobních firem celkem 9 neaplikuje hodnocení plánu rozvoje bezpečnostního povědomí, provedených školení a dalších činností spojených s prohlubováním bezpečnostního povědomí, v rámci pravidelné kontroly a auditu neposuzují soulad bezpečnostních opatření ani neprovádí a nedokumentují pravidelné kontroly dodržování bezpečnostní politiky. Stejný počet společností nevede záznamy o činnostech zpracování OÚ nebo záznamy o všech kategoriích činností zpracování prováděných pro správce. Až 90 % výrobních firem neřeší roli správce dat ani příjemce dat. Stejný počet neplánuje ani zavedení pravidelných školení pro práci s osobními daty. Stejné společnosti také nedisponují přesným popisem procesů, jakým jako správce musí prokazovat vůči UOOU. Další povinnosti jsou neaplikovány z méně než 80 %.

Všech 10 společností používá nástroj pro řízení přístupových oprávnění, kterým zajišťuje řízení oprávnění pro přístup k jednotlivým aplikacím a datům. Všechny společnosti také uplatňují prostředky fyzické bezpečnosti pro zajištění ochrany v rámci objektů zajištěním zvýšené bezpečnosti vymezených prostor, ve kterých jsou umístěna technická aktiva. Každá ze sledovaných firem používá nástroj pro ochranu před škodlivým kódem, který zajistí ověření a stálou kontrolu komunikace mezi vnitřní a vnější sítí a provádí pravidelné aktualizace tohoto nástroje. Všech 10 firem má také zpracovanou kompletní přijímací dokumentaci. Další povinnosti jsou aplikovány u devíti a méně společností. Celkem 19 povinností je vždy u jedné společnosti neaplikovatelných. Nejedná se však vždy o jednu a tu samou společnost.

Zhodnotíme si také, která společnost je na tom nejlépe a která naopak dopadla zle. Vidíme nyní četnosti jednotlivých hodnocení po vynechání nerelevantních povinností (Graf 34.).



Graf 34: Srovnání výrobních podniků.[Zdroj: vlastní zpracování]

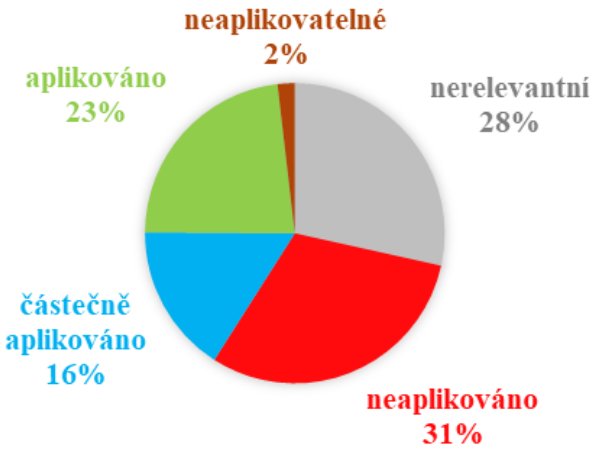
Z grafu je jasně vidět, že vzorek č. 11 je na tom výrazně lépe než ostatní. Má až dvojnásobně méně neaplikovaných povinností a o to více aplikovaných povinností. Naopak nejhůř z výrobních podniků je na tom vzorek č. 28. U tohoto vzorku je více než polovina relevantních povinností neaplikována.

Státní správa

Ve státní správě je problémová oblast Kryptografie, zde celkem 88 % povinností není aplikováno. Dále 75 % povinností z oblasti Pravidelného auditu bezpečnostních opatření k osobním údajům není aplikováno. Dále není aplikováno 71 % povinností z Kontroly a auditu, 60 % z oblasti Řízení rizik a 54 % z Osobních údajů - závazná podniková pravidla. Další oblasti nejsou aplikovány z méně než poloviny.

Ve státní správě si hlídají oblast Vstupních informací osobních údajů - personalistika, aplikují zde 88 % povinností. 80 % povinností je aplikováno v oblastech Ochrana před škodlivým kódem a Řízení přístupových oprávnění. Bez mála 70 % oblastí Log management a Ochrana integrity komunikačních sítí je ve státní správě také aplikována. Další oblasti jsou aplikovány z méně než 63 %.

Celá čtvrtina povinností z oblasti ISMS je ve státní správě neaplikovatelná. Dále je neaplikovatelných 19 % povinností z oblasti Akvizice, vývoje a údržby. Reaktivní a ochranná opatření jsou neaplikovatelná z 13 %. Další oblasti jsou neaplikovatelné z méně než 10 %.



Graf 35: Hodnocení povinností ve státní správě.[Zdroj: vlastní zpracování]

Průměrným hodnocením ve státní správě je hodnocení částečně aplikováno. Nejčastějším hodnocením zde je neaplikováno.

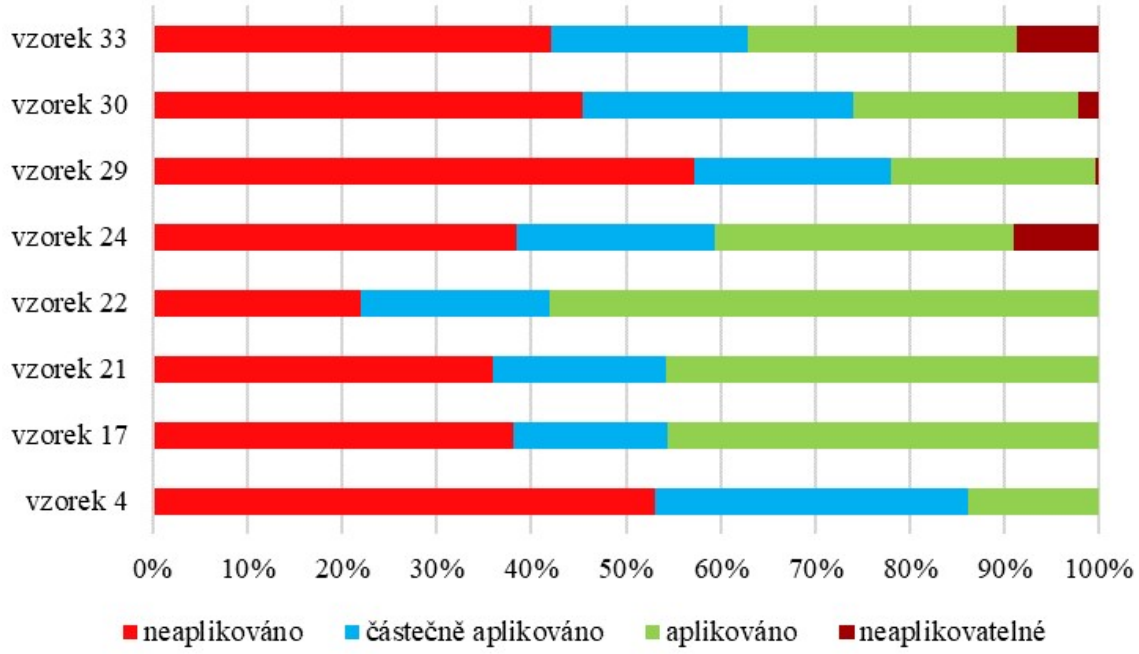
Všech 8 podniků státní správy neprovádí u dodavatelů pravidelné hodnocení rizik a pravidelnou kontrolu zavedených bezpečnostních opatření u poskytovaných služeb a neodstraňují zjištěné nedostatky. Všechny společnosti nestanovují plán rozvoje bezpečnostního povědomí, který obsahuje formu, obsah a rozsah potřebných školení a neurčují osoby provádějící realizaci jednotlivých činností, které jsou v plánu uvedeny. Taktéž všechny podniky nehodnotí účinnost plánu rozvoje bezpečnostního povědomí, provedených školení a dalších činností spojených s prohlubováním bezpečnostního povědomí. Těchto 8 firem také neurčuje pravidla a postupy pro řešení případů porušení stanovených bezpečnostních pravidel ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role (disciplinární řízení). Tyto společnosti v rámci bezpečnostní politiky neřeší používání kryptografické ochrany. Stejně tak tyto společnosti v rámci pravidelné kontroly a auditu neposuzují soulad bezpečnostních opatření, neprovádění a nedokumentují pravidelné kontroly dodržování bezpečnostní politiky a výsledky těchto kontrol nezohledňují

v plánu rozvoje bezpečnostního povědomí a plánu zvládání rizik. Další povinnosti jsou neaplikovány méně něž sedmi společnostmi.

Každý ze státních podniků používá nástroj pro řízení přístupových oprávnění, kterým zajišťuje řízení oprávnění pro přístup k jednotlivým aplikacím a datům, dále zálohují důležitá technická aktiva využitím redundance v návrhu řešení. Všechny tyto podniky používají segmentaci, a to zejména použitím demilitarizovaných zón pro ochranu integrity rozhraní vnější komunikační sítě. Každá společnost také používá nástroj pro ochranu před škodlivým kódem, který zajistí ověření a stálou kontrolu komunikace mezi vnitřní a vnější sítí. Dále taktéž všechny společnosti provádí pravidelné aktualizace nástrojů pro ochranu před škodlivým kódem a zaznamenávají zahájení a ukončení činností technických aktiv pomocí nástroje pro zaznamenávání činnosti informačního/komunikačního systému. Další povinnosti jsou aplikovány méně než sedmi společnostmi.

Je zde také několik neaplikovatelných hodnocení některých povinností. Většinu těchto hodnocení však získaly vzorky č. 24 a č. 33.

Provedeme zde také srovnání všech osmi firem ve státní správě, u kterých bylo provedeno asistované zhodnocení (Graf č. 36).



Graf 36: Srovnání firem ve státní správě.[Zdroj: vlastní zpracování]

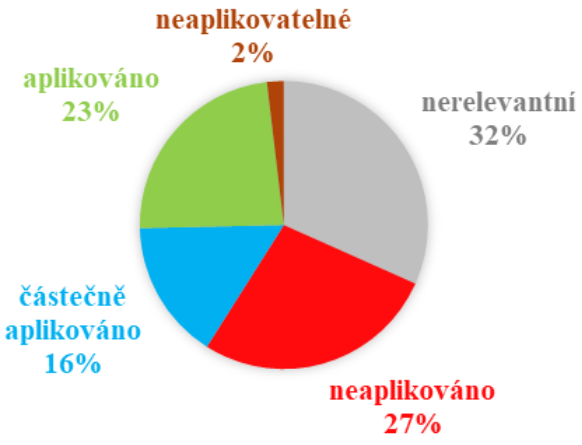
Vidíme, že se opět jeden ze vzorků podstatně odlišuje. Vzorek č. 22 má nejnižší procento neaplikovaných pro něj relevantních povinností a skoro 80 % částečně nebo zcela aplikovaných povinností. Vysoký podíl neaplikovaných řešení mají vzorky č. 29 a č. 4. Vzorek č. 4 má však mnohem více částečně aplikovaných řešení než zcela aplikovaných oproti vzorku č. 29.

Služby

V oboru služeb je na tom nejhůře oblast Kryptografie, celkem 77 % povinností není aplikovaných. Ze 73 % je neaplikovaná oblast Pravidelného auditu bezpečnostních opatření k osobním údajům. Celkem 55 % povinností Kontroly a auditu také není aplikováno. Další oblasti nejsou aplikovány z méně než poloviny.

Z 91 % je řešena a tedy aplikována oblast vstupních informací osobních údajů - personalistika. Dále je aplikovaných povinností 71 % v oblasti Ochrany před škodlivým kódem. Aplikovaných řešení je v oblasti Fyzické bezpečnosti 67 %, v oblasti Ochrany integrity komunikačních sítí 64 %, v oblasti Ověřování identity uživatelů 58 % a v Řízení přístupových oprávnění 55 %. Další oblasti jsou aplikovány z méně než poloviny.

Ve službách je stejně jako ve státní správě neaplikovatelná nejvíce oblast ISMS, zde je to z 18 %. Oblast Detekce kybernetických bezpečnostních událostí je neaplikovatelná ze 14 % a oblast Reaktivních a ochranných opatření od NBÚ je neaplikovatelná ze 9 %. Další oblasti jsou neaplikovatelné z méně něž 7 %.



Graf 37: Hodnocení povinností ve službách.[Zdroj: vlastní zpracování]

Průměrným hodnocením v oboru služeb je hodnocení neaplikováno. Nejčastějším hodnocením zde je nerelevantní.

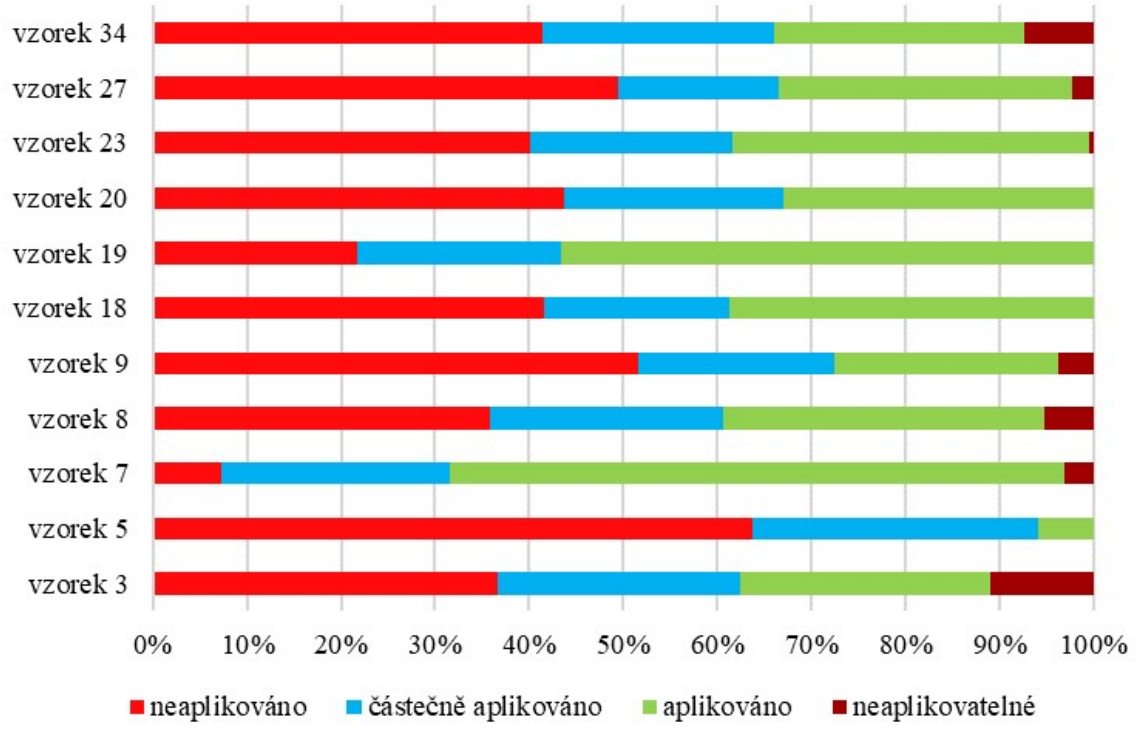
V oblasti služeb není žádná povinnost, která by nebyla aplikována u všech sledovaných firem. Nejvyšší počet hodnocení neaplikováno u jedné povinnosti je 10 z celkových 11. Celkem tedy 10 firem neprovádí u dodavatelů pravidelné hodnocení rizik a pravidelnou kontrolu zavedených bezpečnostních opatření u poskytovaných služeb a zjištěné nedostatky neodstraňuje. Dále nestanovují plán rozvoje bezpečnostního povědomí, který obsahuje formu, obsah a rozsah potřebných školení a nejsou ani určeny osoby provádějící realizaci jednotlivých činností, které jsou v plánu uvedeny. V rámci bezpečnostní politiky neřeší kryptografickou ochranu a nestanovují pro ni úroveň ochrany s ohledem na typ a sílu kryptografického algoritmu, dále pro kryptografickou ochranu nestanovují pravidla kryptografické ochrany informací při přenosu po komunikačních sítích nebo při uložení na mobilní zařízení nebo vyměnitelné technické nosiče dat. V rámci pravidelné kontroly a auditu 10 společností neposuzuje soulad bezpečnostních opatření. Taktéž 10 společností z 11 sledovaných v oblasti služeb při zpracování osobních údajů nevyužívá šifrování osobních údajů. Další povinnosti jsou splněny devíti a méně vzorky.

Ani u aplikovaných povinností nenajdeme žádnou, která by byla aplikována u všech sledovaných vzorků. Celkem 10 firem přiděluje přistupujícím aplikacím samostatný identifikátor a provádí pravidelné aktualizace nástrojů pro ochranu před škodlivým kódem. Společnosti až na jednu identifikují osobní údaje zpracovávané organizací a při zpracování osobních údajů zajišťují schopnost obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů. Společnosti také přistupují k osobním údajů v nestrojové podobě jako k těm strojovým. Dále také kromě jedné společnosti mají zpracovanou kompletní přijímací dokumentaci. Další povinnosti jsou aplikovány u devíti a méně vzorků.

Nejvyšší počet hodnocení neaplikovatelné u jedné povinnosti je dva. Tudíž existuje několik povinností, které nelze aplikovat u 2 firem z 11. Jedná se hlavně o vzorky č. 3 a č. 34. Velká část těchto povinností je z oblasti ISMS a Řízení aktiv. Jsou zde například povinnosti: přidělování a odebírání přístupových oprávnění je prováděno v souladu s politikou řízení přístupu, je používán nástroj pro detekci kybernetických bezpečnost-

ních událostí, který vychází ze stanovených bezpečnostních potřeb a výsledků hodnocení rizik a který zajistí ověření, kontrolu a případné zablokování komunikace mezi vnitřní komunikační sítí a vnější sítí, nejméně jednou za 24 hodin je prováděna synchronizace jednotného systémového času technických aktiv. Tyto a další povinnosti jsou neaplikovatelné u některých společností.

Opět srovnáme všechny vzorky patřící do oblasti služeb (Graf 38.).



Graf 38: Srovnání firem ve službách.[Zdroj: vlastní zpracování]

Na první pohled je na tom nejlépe vzorek č. 7, který má méně než 10 % relevantních povinností neaplikovaných a většinu relevantních povinností má aplikovánu. Vzorek č. 5 je na tom o mnoho hůře. Má naopak méně než 10 % řešení aplikovaných a více než 60% neaplikovaných.

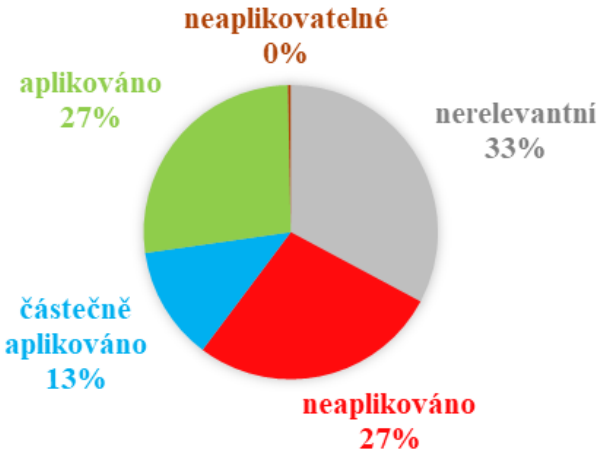
Obchod

V obchodě dělají společnostem nejvíce problémy oblasti Osobních údajů - záznamy o zpracování, Kontroly a auditu a Řízení rizik, neaplikované povinností jsou zde popořadě

z 75 %, 74 % a 72 %. Dále je 60 % povinností neaplikovaných v oblastech Kryptografie a Pravidelném auditu bezpečnostních opatření k osobním údajům. Další oblasti jsou neaplikovány z méně než 54 %

Velká většina povinností (90 % a 88 %) Fyzické bezpečnosti a Ochrany před škodlivým kódem je v obchodních společnostech aplikována. 80 % povinností je aplikováno v oblastech Ochrany integrity komunikačních sítí a Vstupních informací osobních údajů - personalistika. V oblastech Ověřování identity uživatelů a Řízení přístupových oprávnění je aplikováno 73 % povinností. Další oblasti jsou aplikovány z méně než 71 %.

Neaplikovatelných povinností je v obchodních společnostech nejvíce v oblasti Řízení aktiv, jsou to však pouze 4 %. Bez mála 2 % povinností jsou neaplikovatelná v oblastech Řízení přístupu a bezpečného chování uživatelů a Bezpečnosti lidských zdrojů. Další oblasti neobsahují žádné neaplikovatelné povinnosti.



Graf 39: Hodnocení povinností v obchodě.[Zdroj: vlastní zpracování]

Průměrným hodnocením ve společnostech, které se zabývají obchodem, je hodnocení nerelevantní. Stejně tak je to nejčastější hodnocení v tomto oboru.

V oboru obchodu jsme našli celkem 18 povinností, které jsou neaplikovány u všech sledovaných vzorků spadajících do obchodu. Celkem 10 povinností, které nejsou aplikovány u všech firem patří do oblasti Osobních údajů a OÚ - záznamy o zpracování. Mimo povinnosti spadající do témat osobních údajů jsou neaplikovány následující relevantní

povinnosti. Všechny sledované společnosti v oblasti obchodu nezvažují zranitelnosti související s nedostatečnou ochranou ICT, nevhodnou bezpečnostní architekturou, nedostatečnou mírou nezávislé kontroly, neschopností včasného odhalení pochybení ze strany zaměstnanců. Společnosti nestanovují plán rozvoje bezpečnostního povědomí. Dále také neprovádí výměnu a předávání informací na základě písemných smluv, jejichž součástí je ustanovení o bezpečnosti informací, s ohledem na klasifikaci aktiv. V rámci bezpečnostní politiky neřeší kryptografickou ochranu. Dále nepoužívají nástroj pro zaznamenávání činností ICT. V rámci pravidelné kontroly a auditu neposuzují soulad bezpečnostních opatření, neprovádí a nedokumentují pravidelné kontroly dodržování bezpečnostní politiky a výsledky těchto kontrol nejsou zohledněny v plánu rozvoje bezpečnostního povědomí a plánu zvládání rizik.

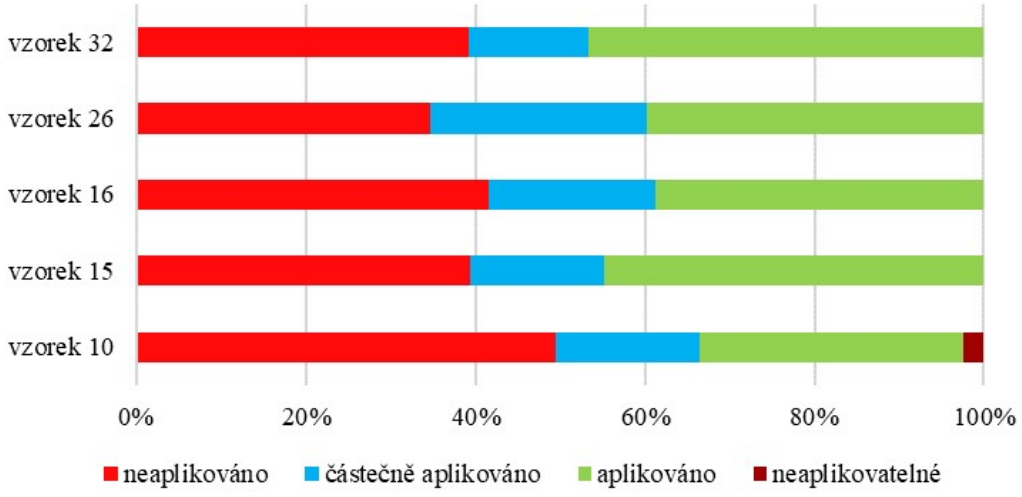
Společnosti v tomto oboru všechny najednou aplikují 32 povinností. Existuje tedy 32 povinností, které aplikují všechny společnosti z oblasti obchodu. Všechny tyto povinnosti jsou z oblastí Řízení provozu a komunikací, Řízení přístupových oprávnění, Akvizice, vývoj a údržba, Aplikační bezpečnost, Fyzická bezpečnost, Ochrana integrity komunikačních sítí, Ochrana před škodlivým kódem a Osobní údaje. Například všechny společnosti provádí pravidelné zálohování a prověřování použitelnosti provedených záloh, omezují přidělování administrátorských oprávnění, provádí bezpečnostní testování změn systémů před jejich zavedením do provozu, předcházejí poškození, krádeži nebo kompromitaci aktiv nebo přerušení poskytování služeb nebo je u všech firem používán nástroj pro ochranu před škodlivým kódem, který zajistí ověření a stálou kontrolu pracovních stanic.

Dále tyto společnosti přijímají nezbytná opatření k zamezení poškození a zásahům do vymezených prostor, kde jsou uchovány informace a umístěna technická aktiva, pro ochranu integrity rozhraní vnější komunikační sítě mají zavedenou segmentaci zejména použitím demilitarizovaných zón. Také je zajištěna bezpečnost vývojového prostředí a zároveň je zajištěna ochrana používaných testovacích dat, jsou zavedena bezpečnostní opatření potřebná pro bezpečné používání mobilních zařízení, případně i bezpečnostní opatření spojená s využitím technických zařízení, kterými povinná osoba nedisponuje. Tyto a mnoho dalších povinností jsou aplikovány všemi vzorky v oboru obchodu.

Pouze 4 povinnosti získaly hodnocení neaplikovatelné a to u jednoho vzorku. Vzo-

rek č. 10 jako jediný v oblasti obchodu není schopen aplikovat následující povinnosti. Nemůže přidělování a odebírání přístupových oprávnění provádět v souladu s politikou řízení přístupu, nelze určit bezpečnostní role: garant/vlastník aktiva, nelze stanovit pravidla ochrany, nutná pro zabezpečení jednotlivých úrovní aktiv tím, že jsou zavedena pravidla ochrany odpovídající úrovni aktiv, jsou určeny způsoby pro spolehlivé smazání nebo ničení technických nosičů dat s ohledem na úroveň aktiv, nelze zajistit změnu přístupových oprávnění při změně postavení uživatelů, administrátorů nebo osob zastávajících bezpečnostní role.

Porovnáme také společnosti, které se věnují obchodu (Graf 40.). Vidíme 5 vzorků z oblasti obchodu, které jsme analyzovali.



Graf 40: Srovnání obchodních podniků.[Zdroj: vlastní zpracování]

Ze všech oborů jsou v obchodě nejmenší rozdíly mezi vzorky. I přesto můžeme říci, že vzorek č. 10 je na tom nejhůře, má skoro polovinu relevantních povinností neaplikovánu a jako jediný má neaplikovatelné povinnosti. Ostatní vzorky jsou na tom velice podobně. Nejméně neaplikovaných řešení je však u vzorku č. 26.

4.6 Hodnocení konkrétního vzorku

V této části provedeme detailní hodnocení vybraného vzorku. Analyzovanou společností bude vzorek č. 5. V první části si uvedeme základní informace o společnosti a dále se zaměříme na výsledky asistovaného zhodnocení.

4.6.1 Informace o společnosti

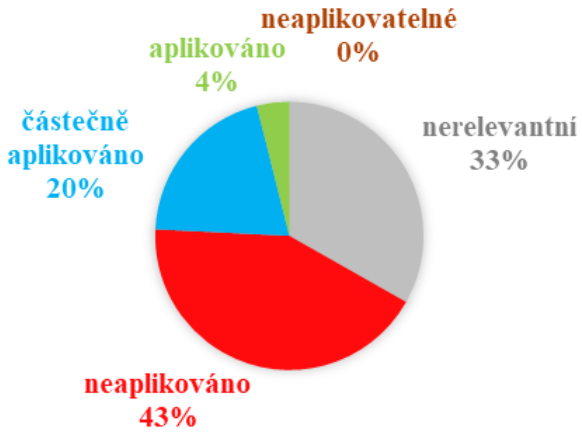
Společnost vznikla v roce 1997 a začínala jako servis pro telekomunikační hardware. Od té doby se společnost rozrůstala a nabírala nové a nové klienty. Postupně rozšiřovala i své portfolio služeb o ERP systémy, cloudová úložiště a CRM systémy.

Jde o společnost, která spadá do kritické informační infrastruktury. Tato společnost podniká v oblasti služeb a to konkrétně v ICT (informační a komunikační technologie). Jedná se o střední společnost, zaměstnávají okolo 50–100 zaměstnanců.

Společnost nyní nabízí tvorbu podnikových IT systémů zákazníkům na míru, dále různé telekomunikační systémy nebo cloudová úložiště. Dále společnost provádí GDPR školení a audity, webináře o IT bezpečnosti a další služby.

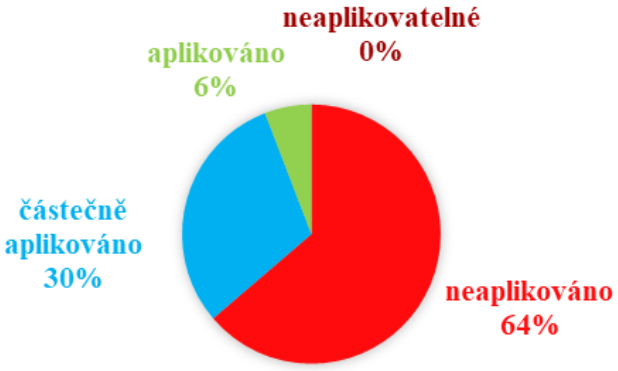
4.6.2 Hodnocení plnění povinností

V této části se podíváme na hodnocení všech povinností, které byly u vybrané společnosti sledovány. Stejně jako u všech dalších vzorků jsme hodnotili 256 povinností, rozdělených do několika oblastí. Následující graf (Graf č. 41) zachycuje výsledné četnosti jednotlivých hodnocení. Jak můžeme vidět, celkem 33 % povinností bylo u společnosti uznáno jako nerelevantních, to znamená celkem 85 řešení. V této společnosti nebyla nalezena ani jedna povinnost jako neaplikovatelná. Průměrné hodnocení a stejně tak nejčastější hodnocení u této společnosti je neaplikováno.



Graf 41: Hodnocení povinností vzorku č. 5.[Zdroj: vlastní zpracování]

Nyní nebudeme brát v úvahu povinnosti, které jsou pro společnost nerelevantní. Zbylé relevantní povinnosti byly hodnoceny a výsledky můžeme vidět níže (Graf č. 42).



Graf 42: Hodnocení relevantních povinností vzorku č. 5.[Zdroj: vlastní zpracování]

Drtivých 64 % povinností, které jsou pro společnost relevantní a měla by je tedy implementovat, jsou neaplikovány. Společnost částečně 30 % a pouhých 6 % řešení aplikuje zcela. Jak víme, jedná se o společnost podnikající v oblasti služeb, to znamená, že většinu rizik spojených s neaplikováním povinností přenáší také na své klienty.

4.6.3 Hodnocení oblastí povinností

Nyní se zaměříme na hodnocení jednotlivých oblastí jako celků. Uvedeme oblasti, které jsou vždy z velké části nerelevantní / neaplikovány / částečně aplikovány / aplikovány / neaplikovatelné.

Tabulka 11: Nerelevantní oblasti pro vzorek č. 5.[Zdroj: vlastní zpracování]

Oblast
Bezpečnost ICS/SCADA
Kontrola a audit
OÚ v IS provozovaných v REHAU
Posouzení vlivu dopadu na ochranu osobních údajů dle č. 35
Pravidelný audit bezpečnostních opatření k OÚ
Přenositelnost údajů
Reaktivní a ochranná opatření od NBÚ
Vstupní informace OÚ – personalistika

Veškeré oblasti, které jsou v tabulce (Tabulka č. 11) jsou pro společnost nerelevantní, to znamená, že všechny povinnosti z těchto oblastí považujeme za nerelevantní. Další tabulka (Tabulka 12.) obsahuje oblasti, ze kterých společnost nemá aplikovánu ani jednu povinnost, jsou tedy zcela neaplikované.

Tabulka 12: Oblasti, které vzorek č. 5 vůbec neaplikuje.[Zdroj: vlastní zpracování]

Oblast
Detekce kybernetických bezpečnostních událostí
ISMS
OÚ – kodexy chování
OÚ – závazná podniková pravidla
OÚ – záznamy o zpracování
Řízení přístupových oprávnění
Řízení rizik
SIEM

Dále neaplikuje z 92 % oblast Log management, celých 64 % povinností není aplikováno ani v oblasti Řízení aktiv, 63 % v oblasti BCM a 58 % v oblasti Bezpečnosti lidských zdrojů. Další oblasti jsou neaplikovány z méně než poloviny.

Následující tabulka (Tabulka č. 13) udává oblasti, které společnost v určité míře aplikuje, tedy zcela aplikuje některé povinnosti v těchto oblastech. To, kolik povinností v dané oblasti aplikuje, je také vidět z tabulky. V ostatních oblastech, které nejsou uvedeny v tabulce, společnost nemá žádnou povinnost, kterou by aplikovala.

Tabulka 13: Podíl aplikovaných povinností u vzorku č. 5.[Zdroj: vlastní zpracování]

Oblast	Aplikováno
Ochrana před škodlivým kódem	40 %
Aplikační bezpečnost	33 %
Řízení přístupu a bezpečné chování uživatelů	27 %
Ověřování identity uživatelů	20 %
Řízení provozu a komunikací	11 %
Osobní údaje	2 %

Oblasti, které jsou uvedeny v tabulce (Tabulka č. 14) jsou aplikovány částečně. Počet povinností, které jsou v dané oblasti částečně aplikovány je uvedeno taktéž v tabulce. Další oblasti, které v tabulce nevidíme, nemají žádné řešení s hodnocením částečně aplikováno.

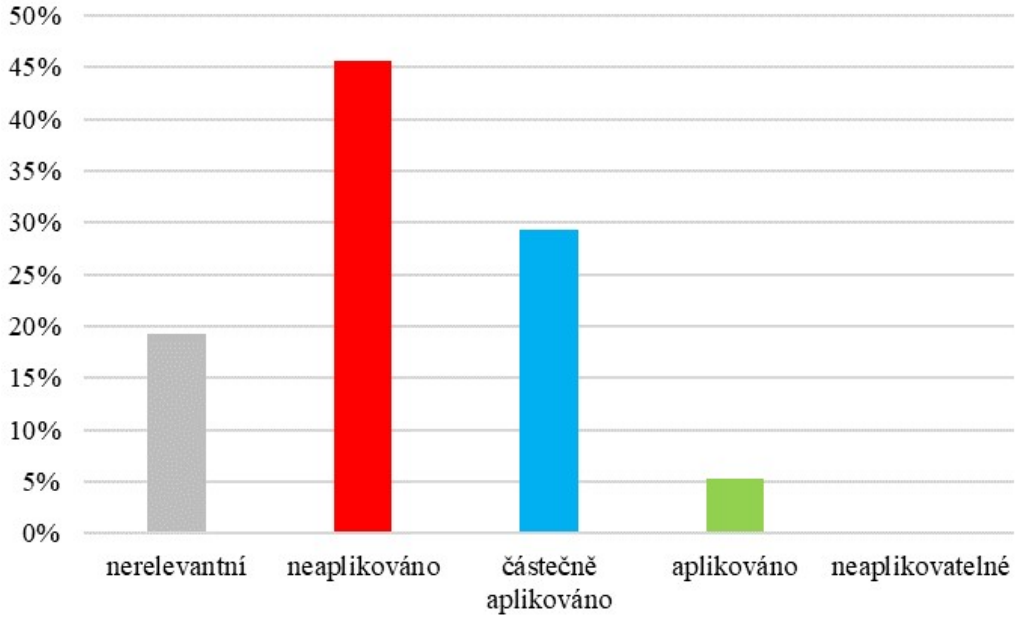
Tabulka 14: Podíl částečně aplikovaných povinností u vzorku č. 5.[Zdroj: vlastní zpracování]

Oblast	Částečně aplikováno
Ochrana integrity komunikačních sítí	80 %
Akvizice, vývoj a údržba	75 %
Aplikační bezpečnost	67 %
Fyzická bezpečnost	67 %
Ochrana před škodlivým kódem	60 %
Řízení provozu a komunikací	53 %
Incident handling	50 %
Ověřování identity uživatelů	40 %
Řízení přístupu a bezpečné chování uživatelů	36 %
Řízení aktiv	36 %
Bezpečnost lidských zdrojů	33 %
Kryptografie	33 %
Řízení dodavatelů	29 %
Zajištění dostupnosti	20 %
BCM	13 %
Log management	8 %
Osobní údaje	5 %

Žádná z povinností, které byly sledovány, nemá hodnocení neaplikovatelné. Společnost má tedy veškeré povinnosti buď aplikovány, aplikovány částečně, neaplikovány nebo nerelevantní.

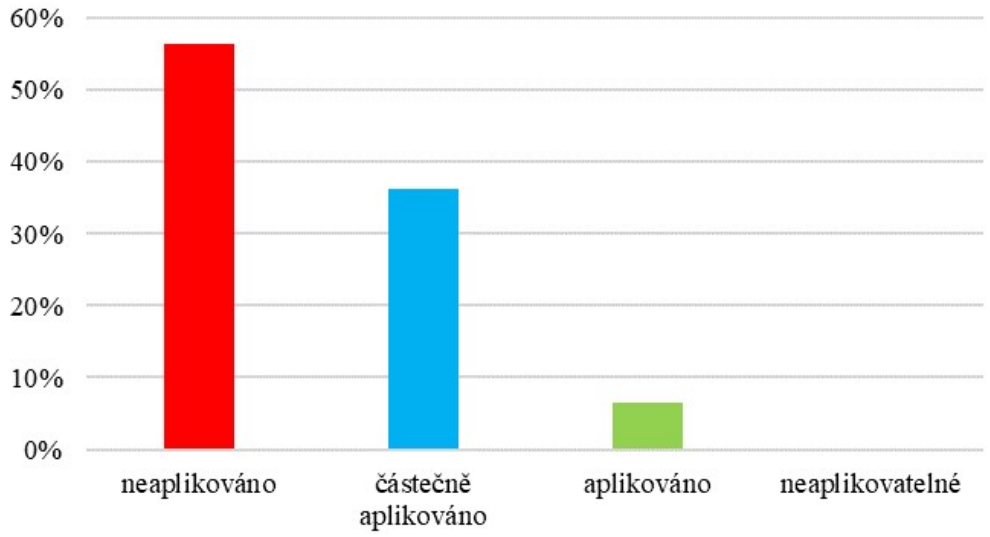
4.6.4 Hodnocení povinností spadajících do KII

Jak jsme již zmínili, vzorek č. 5 je společností, která spadá do kritické informační infrastruktury. V této části se podíváme, jak plní povinnosti, které souvisí s kritickou informační infrastrukturou a tato společnost by je tedy měla aplikovat.



Graf 43: Hodnocení KII povinností vzorku č. 5.[Zdroj: vlastní zpracování]

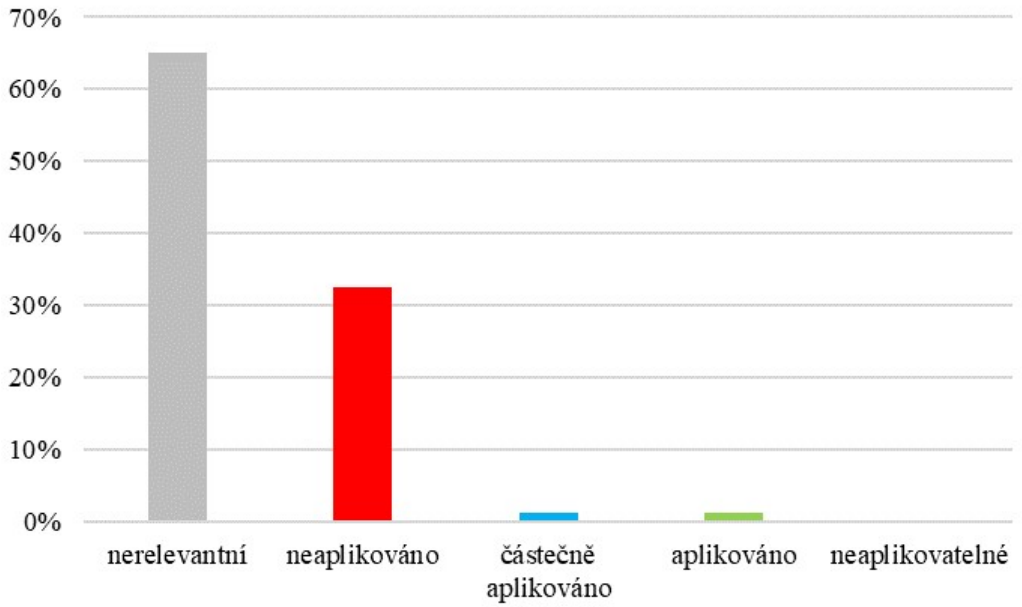
Z grafu (Graf č. 43) je patrné, že je skoro 20 % povinností spadajících do oblasti kritické informační infrastruktury nerelevantních. Dále budeme tyto povinnosti ignorovat. Společnost neaplikuje více než polovinu relevantních povinností z oblasti KII. Dále můžeme vidět (Graf č. 44), že zbylé povinnosti aplikuje ve velké míře pouze částečně (36 %) a pouze 7 % povinností aplikuje zcela. Pro společnost, která spadá do kritické informační infrastruktury je takové hodnocení velice špatné.



Graf 44: Hodnocení relevantních KII povinností vzorku č. 5.[Zdroj: vlastní zpracování]

4.6.5 Hodnocení povinností spadajících do GDPR

Společnost nabízí mnoho služeb v oblasti GDPR. Nabízí školení nebo audit. Dále nabízí poradenství a konzultace. Klientům je schopna implementovat GDPR nebo zařídit outsourcing Pověřence, kterého GDPR specifikuje. Zajímá nás tedy, jak taková společnost sama plní povinnosti, jejich implementaci vlastně nabízí. Zjištění je však zcela kritické. Ve společnosti je hodnoceno 65 % povinností spadajících do GDPR jako nerelevantní. Dalších 33 % povinností je neaplikováno a pouhé jedno procento je aplikováno částečně a jedno procento aplikováno zcela.



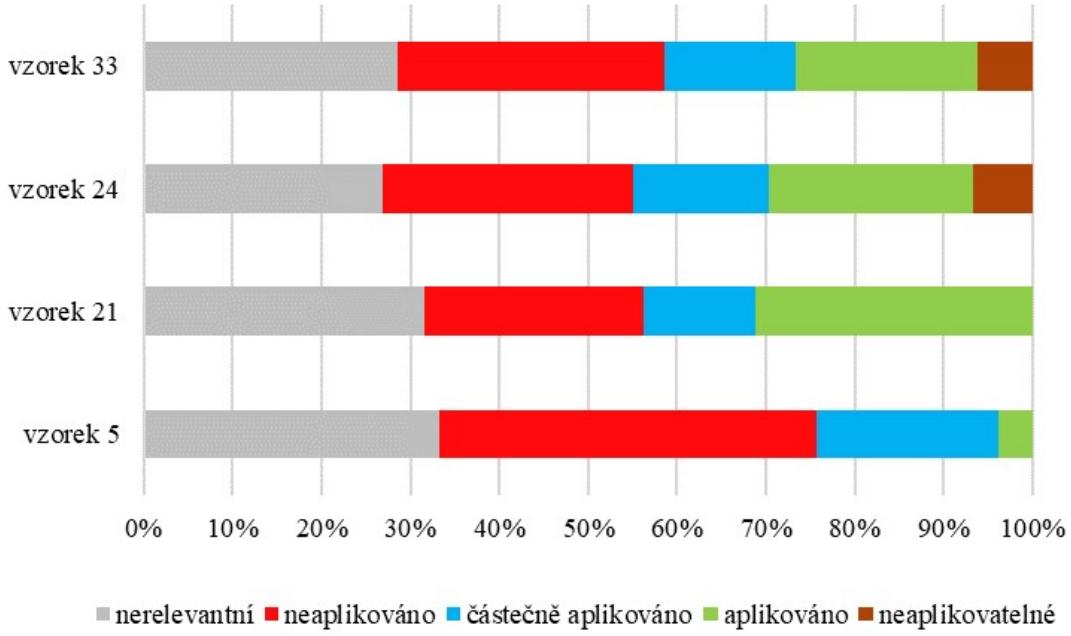
Graf 45: Hodnocení GDPR povinností vzorku č. 5.[Zdroj: vlastní zpracování]

Pokud vezmeme v potaz pouze relevantní povinnosti, tak společnost neaplikuje skoro 93 % a aplikuje pouze 7 % částečně nebo zcela. Společnost tedy nabízí služby v oblasti, kterou nemá sama v pořádku.

Graf 46: Hodnocení relevantních GDPR povinností vzorku č. 5.[Zdroj: vlastní zpracování]

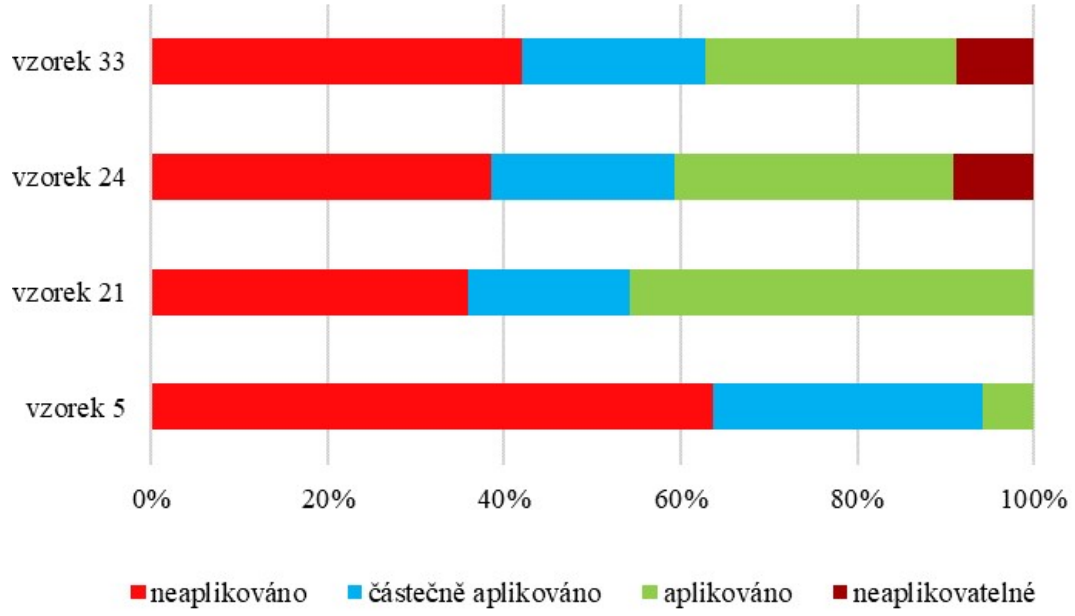
4.6.6 Porovnání s podobnými subjekty

V této části porovnáme analyzovaný subjekt se společnostmi stejného typu. Ve skupině se zhruba stejným počtem zaměstnanců jsou další tři společnosti. A co se týče předmětu podnikání, ve službách je dalších 10 subjektů. Vzorek č. 5 je však jediný vzorek své velikosti podnikající v oblasti služeb. Jedná se o subjekt kritické informační infrastruktury, což jsou i další 4 vzorky.



Graf 47: Hodnocení podobně velkých vzorků.[Zdroj: vlastní zpracování]

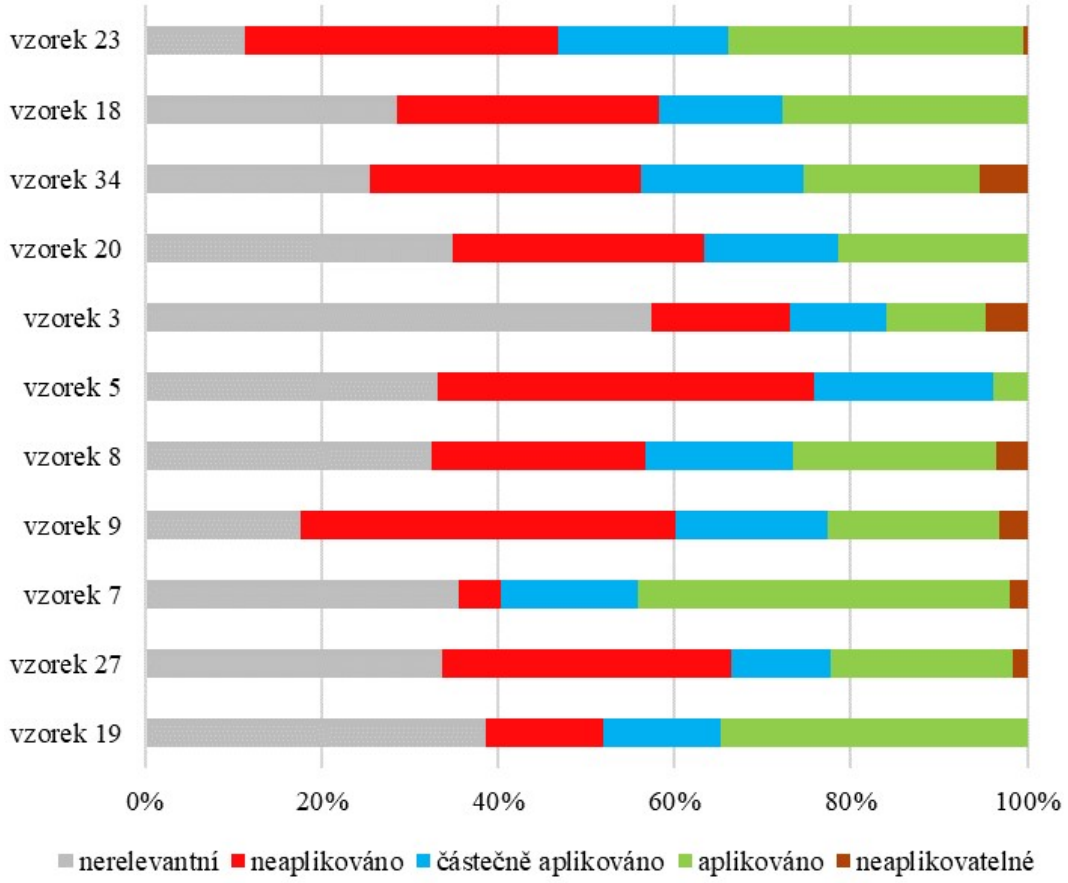
Námi analyzovaný vzorek č. 5 má největší počet nerelevantních povinností mezi subjekty stejné velikosti (Graf č. 47). Na dalším grafu (Graf č. 48) zobrazíme už jen relevantní povinnosti. Vzorek je v této skupině rozhodně nejhorší. Má skoro dvakrát více neaplikovaných povinností. Stejně jako vzorek č. 21 nemá žádné neaplikovatelné povinnosti, ale aplikovaných povinností má zhruba pětinu oproti ostatním vzorkům. Má pouze více částečně aplikovaných povinností než ostatní vzorky.



Graf 48: Hodnocení relevantních povinností podobně velkých vzorků.[Zdroj: vlastní zpracování]

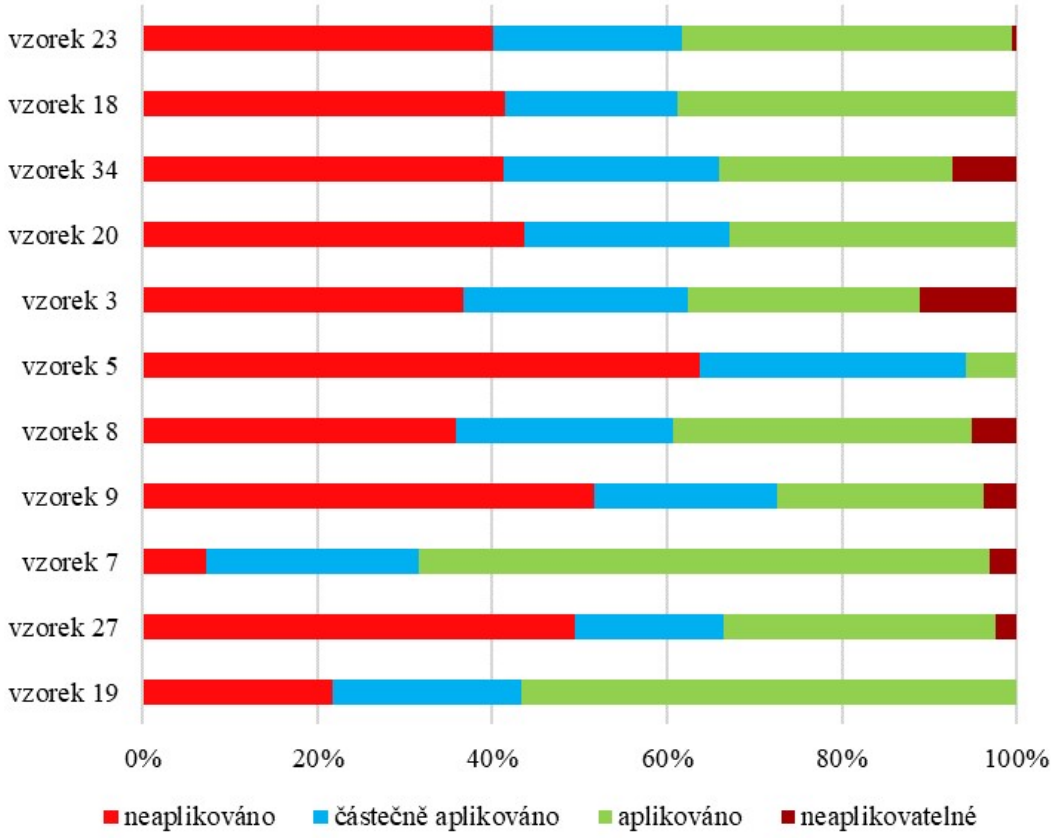
Ve skupině středních podniků (50–100 zaměstnanců) je průměrně 30 % nerelevantních, 31 % neaplikovaných, 16 % částečně a 20 % zcela aplikovaných a 3 % neaplikovatelných povinností. Vzorek č. 5 má tedy o 8 nerelevantních povinností, o 29 neaplikovaných povinností a o 12 částečně aplikovaných povinností více, než je průměr pro tuto velikost. Dále má o 40 aplikovaných povinností méně oproti průměrnému počtu v této velikostní skupině.

Nyní se podívejme, jak je na tom vzorek v porovnání se společnostmi podnikajícími v oblasti služeb (Graf č. 49). Zde analyzovaná společnost (vzorek č. 5) nemá již největší počet nerelevantních povinností. Mnohem více jich má vzorek č. 3. Až na vzorky č. 23 a č. 9 mají všechny velmi podobný počet nerelevantních povinností.



Graf 49: Hodnocení povinností vzorků v oboru služeb.[Zdroj: vlastní zpracování]

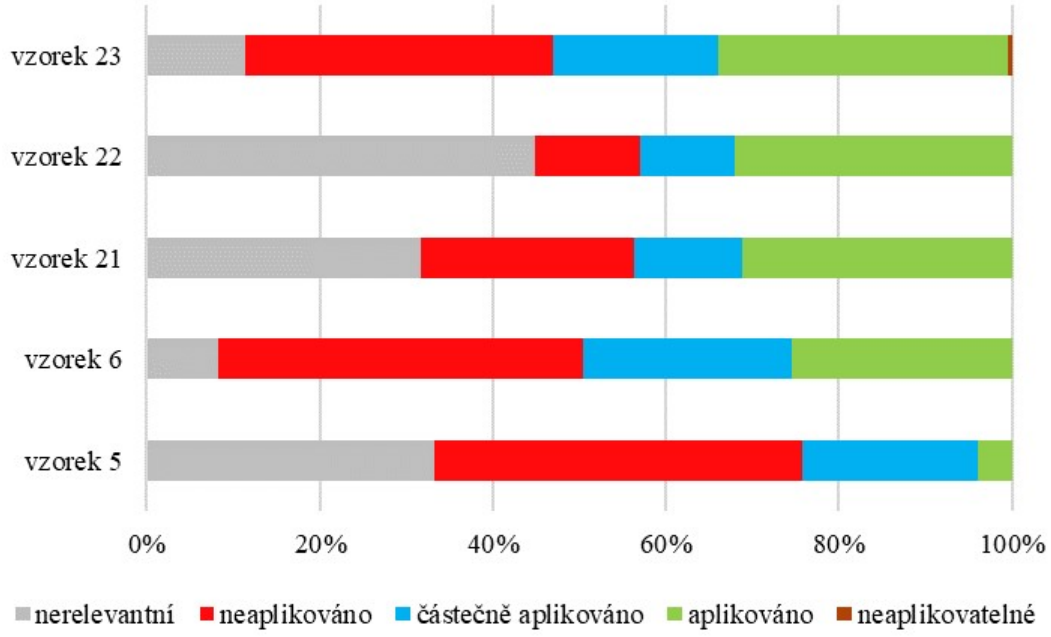
Dále vidíme hodnocení relevantních povinností (Graf č. 50). Jak můžeme vidět i zde má největší počet svých relevantních povinností neaplikováno vzorek č. 5. Má také nejméně aplikovaných povinností. Spolu se vzorky č. 18, č. 20 a č. 19 nemá žádné neaplikovatelné povinnosti.



Graf 50: Hodnocení relevantních povinností vzorků v oboru služeb.[Zdroj: vlastní zpracování]

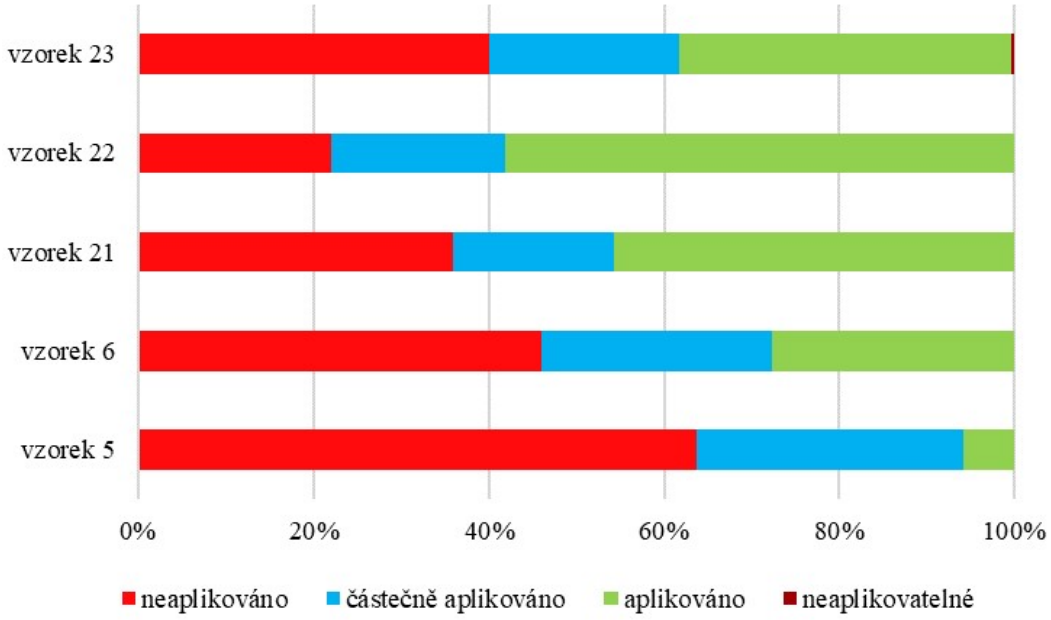
Ve skupině společností podnikajících v oblasti služeb je průměrně 32 % nerelevantních, 27 % neaplikovaných, 16 % částečně a 23 % zcela aplikovaných a 2 % neaplikovatelných povinností. Vzorek č. 5 má o 4 nerelevantní povinnosti, o 39 neaplikovaných povinností a o 12 částečně aplikovaných povinností více, než je průměr pro odvětví služeb. Dále má o 50 aplikovaných povinností méně oproti průměrnému počtu ve službách.

Jelikož se jedná o subjekt patřící do kritické informační infrastruktury, podíváme se také na to, jak si v této oblasti vede oproti dalším KII subjektům. Jak můžeme vidět z grafu (Graf č. 51) počty nerelevantních povinností jsou velice různé.



Graf 51: Hodnocení povinností vzorků spadajících do KII.[Zdroj: vlastní zpracování]

Vzorek č. 5 má opět největší podíl relevantních neaplikovaných povinností a nejmenší počet aplikovaných. Má nejvíce částečně aplikovaných řešení. Stejně jako další tři subjekty nemá ani jednu neaplikovatelnou povinnost.



Graf 52: Hodnocení relevantncích povinností vzorků spadajících do KII.[Zdroj: vlastní zpracování]

Společnosti, které spadají do KII mají průměrně 26 % nerelevantních povinností, 31 % neaplikovaných povinností, 17 % částečně a 25 % zcela aplikovaných a žádnou neaplikovatelnou povinnost. Náš analyzovaný subjekt vykazuje o 19 nerelevantních povinností, o 29 neaplikovaných povinností a o 7 částečně aplikovaných povinností více, než je průměr pro společnosti patřící do KII. Také má o 55 aplikovaných povinností méně oproti průměrnému počtu v KII.

4.7 Asistovaná zhodnocení a systémová integrace

Systémový integrátor velmi často provádí i studie proveditelnosti. Stejně tak by mohl provádět ve společnosti asistovaná zhodnocení. Takové asistované zhodnocení by měl provést před tím, než bude ve společnosti integrovat systém, data nebo i jiné technologie.

Jelikož systémový integrátor ke své práci potřebuje znát detailně danou společnost, její procesy, technologie, dodavatelský řetězec apod., je žádoucí a dle mého názoru i efektivní, aby prováděl i asistované zhodnocení. Takto mohou společnosti snížit náklady, čas i riziko úniku informací.

Náklady společnosti mohou snížit z toho důvodu, že zaplatí pouze systémového integrátora a ne dvě různé osoby/společnosti na systémovou integraci a asistované zhodnocení. Zároveň se sníží i čas takových operací. Společnost by mohla systémového integrátora se vším seznámit a čas, který by věnovala osobě/společnosti, kterou seznámí se všemi oblastmi asistovaného zhodnocení, může využít jinak. To také souvisí s možným únikem informací. Jelikož by systémový integrátor a analytik provádějící asistované zhodnocení byl jednou osobou/společností, nebudeme informace šířit tolika směry.

Takové propojení může pomoci i z toho důvodu, že se systémový integrátor může dozvědět zásadní informace z asistovaného zhodnocení, které by jinak mohl přehlédnout a naopak. Analytik provádějící asistované zhodnocení může získat informace, které mu mohou být nápomocné při systémové integraci.

4.8 Ekonomické zhodnocení této práce

Jelikož je tato práce speciální analýzou, která se obvykle neprovádí, ocenění takové práce je čistě orientační a vytvoříme ho na základě obdobných analýz. Pro informaci zde uvedeme i orientační finanční ohodnocení asistovaného zhodnocení.

Cena asistovaného zhodnocení je velice individuální a výše závisí na mnoha faktorech: velikost subjektu, počet schůzek, počet poradenských schůzek, rozsah dodatečné dokumentace apod. Průměrná cena asistovaného zhodnocení se pohybuje okolo 200 000 Kč. K tomu se obvykle přidávají poradenské služby realizačního týmu. Tyto služby se cení za jednu člověkohodinu. Jednotková cena je tedy v průměru 1 625 Kč. Uvedené ceny jsou bez DPH. Detail vidíme v tabulce (Tabulka č. 15).

Tabulka 15: Cena vypracování asistovaného zhodnocení.[Zdroj: vlastní zpracování dle: 22]

Služba	Cena bez DPH	DPH (21 %)	Cena s DPH
Vypracování asistovaného zhodnocení	200 000 Kč	42 000 Kč	242 000 Kč
Jednotková cena poradenských služeb členů realizačního týmu za jednu člověkohodinu	Cena analýzy bez DPH	DPH (21 %)	Cena analýzy s DPH
Poradenství	1 625 Kč	341,25 Kč	1 966,25 Kč

Cena analýz v rozsahu této práce se pohybuje obvykle okolo 100 000 Kč. Jednotková cena za člověkohodinu autora této práce je 700 Kč. Nejsme schopni odhadnout dobu, za kterou byla tato práce vypracována a proto budeme brát v úvahu počet stran A4 místo hodin strávených nad touto prací. V návrhové části je 68 stran A4. Uvedené ceny jsou bez DPH. Detailní rozpis vidíme v tabulce (Tabulka č. 16).

Tabulka 16: Cena vypracování analýzy tohoto typu.[Zdroj: vlastní zpracování]

Jednotkové ceny	Jednotková cena za stranu A4 bez DPH	DPH (21 %)	Jednotková cena za stranu A4 s DPH
-	700 Kč	147 Kč	847 Kč
Počet stran A4	Cena analýzy bez DPH	DPH (21 %)	Cena analýzy s DPH
68	47 600 Kč	9 996 Kč	57 596 Kč

4.9 Závěrečné shrnutí a doporučení

Tato práce nám podává zásadní zjištění. Útvary odpovědné za řízení společností, které připadají ke vzorkům v této práci, by měli v první řadě podstoupit školení. Je důležité, aby pochopili důležitost kybernetické a informační bezpečnosti a uvědomili si, co jim hrozí a co mohou způsobit. Jakmile budou znát závažnost situace, budou své společnosti vést k lepšímu naplňování povinností z oblasti kybernetické a informační bezpečnosti.

Veškeré zkoumané vzorky jsou z mého pohledu v nevyhovujícím stavu a je více než žádoucí, aby se tento stav změnil. Nezbývá jen doufat, že se nejedná o reprezentativní vzorky a existují společnosti, jejichž hodnocení není takto závažné.

Na základě vyhodnocených dat je zřejmé, že neexistuje jednotný přístup k tomu, jak by společnosti měly implementovat povinnosti z kybernetické a informační bezpečnosti v praxi. Každá společnost se zaměřuje na jiné oblasti z asistovaného zhodnocení a nevidí kybernetickou a informační bezpečnost jako celek a z komplexního úhlu pohledu. Proto se vytváří Metodika asistovaného zhodnocení [21]. Tato metodika popisuje důkladně všechny povinnosti, které ukládá legislativa popsaná v této práci a mnoho dalších. Jsou v ní uvedeny pokyny k vypracování asistovaného zhodnocení, detailní popis jednotlivých částí a oblastí.

ZÁVĚR

V této části shrneme obsah práce a zhodnotíme dosažení a naplnění stanovených cílů. V rámci teoretické části byly popsány zásadní normy a jejich instituce z oblasti kybernetické a informační bezpečnosti. Dále je popsána legislativa, na jejimž základe stojí asistované zhodnocení. V této kapitole najdeme také výklad nejdůležitějších pojmů, které jsou potřebné k pochopení dalšího textu práce.

Ve druhé kapitole jsme se seznámili s asistovaným zhodnocením. Popsali jsme data, jejich získání a proces před zahájením analýz. Dále jsme se zaměřili na nejdůležitější podmínky pro vypracování asistovaného zhodnocení. V této kapitole jsou také uvedeny části asistovaného zhodnocení, tedy co všechno by v něm nemělo chybět a jak reálně vypadá. Oblasti povinností, které se v dotazníku pro asistované zhodnocení vyskytují jsou popsány taktéž v této kapitole. Na závěr této části je uvedeno proč a kdy by mělo být vypracováno asistované zhodnocení a z čeho se takové hodnocení skládá.

Stěžejní část práce je návrhová čtvrtá kapitola. Ta se věnuje analýze získaných vzorků asistovaného zhodnocení. V první fázi byla provedena souhrnná analýza všech vzorků, zjistili jsme tak stav, ve kterém se nachází sledované společnosti a můžeme díky tomu soudit stav, v jakém je nejspíš většina společností a organizací na území ČR. Poté jsme zkoumali data z pohledu označení povinností příznaky KII, VIS nebo GDPR, dle oblastí povinností, dle velikosti vzorků nebo oboru jejich podnikání. Tato kapitola také obsahuje detailní průzkum hodnocení konkrétního vybraného vzorku. Závěrem je uvedeno zamyšlení nad spojením asistovaného zhodnocení a systémové integrace. Dále pak doporučení a zásadní informace, získaná díky této práci.

Stanovených cílů této práce bylo tedy dosaženo. Práce byla zadáním skutečných potřeb a výstup bude sloužit jako doplňující dokument pro společnosti, které odpovídají vzorkům v této práci. Diplomová práce může posloužit jako příručka nebo podklad k analyzování většího množství vzorků. Analytik může využít nastavené pohledy a způsoby porovnávání a své získané vzorky srovnávat obdobným způsobem. Práce je také vhodná, pokud auditor nebo analytik asistovaného zhodnocení potřebuje srovnání s jinou podobnou společností. Výsledky takovýchto analýz mohou být společnostem, pro které

se vypracovává asistované zhodnocení, předloženy jako doplňující analýzy. Tato práce obsahuje také detailní analýzu konkrétního vzorku, která může sloužit jako příručka pro analýzy dalších vzorků.

Díky vlastnostem, které jsou ze vzorků asistovaného zhodnocení zjištěny a v této práci popsány, budou auditoři nebo osoby pověřené vypracováním asistovaného zhodnocení schopni identifikovat problémové oblasti nebo konkrétní povinnosti, na které je třeba se zaměřit.

Tato diplomová práce slouží také jako jakýsi indikátor stavu kybernetické a informační bezpečnosti ve společnostech v ČR. Asistovaná zhodnocení použitá v této diplomové práci byla získána z reálných subjektů podnikajících na území ČR. Zjištění z této práce je zprávou pro společnosti v ČR, která by měla vyvolat tlak a donutit společnosti a jiné subjekty ke zlepšení, a hlavně řešení situace v oblasti kybernetické a informační bezpečnosti. Práce má motivovat k nepřehlížení stavu bezpečnosti ve společnostech a dalších subjektech v našem státě.

Jelikož je asistované zhodnocení relativně novým pojmem, tato práce jej může přiblížit veřejnosti. Práce také potvrzuje potřebu Metodiky asistovaného zhodnocení [21].

SEZNAM POUŽITÝCH ZDROJŮ

[1] ONDRÁK, Viktor. *Management informační bezpečnosti* [přednáška]. Brno, 2014.

[2] ISO/IEC 27000. *Information technology — Security techniques — Information security management systems — Overview and vocabulary.* 5. vydání. Švýcarsko: Mezinárodní organizace pro normalizaci, 2018.

[3] ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. *Problematika ISMS v manažerské informatice.* Brno: Akademické nakladatelství CERM, 2013. ISBN 978-80-7204-872-4.

[4] SEDLÁK, Petr. *Kybernetická bezpečnost: Obecně* [přednáška]. Brno, 2017.

[5] Česká agentura pro standardizaci [online]. 2019 [cit. 2019-02-18]. Dostupné z: http://www.agentura-cas.cz/

[6] Draft NISTIR 7298. *Glossary of Key Information Security Terms.* 3. revize. U.S. Department of Commerce: National Institute of Standards and Technology, 2018.

[7] NIST SP 800-12. *An Introduction to Information Security.* 1. revize. U.S. Department of Commerce: National Institute of Standards and Technology, 2017.

[8] Draft NIST SPECIAL PUBLICATION 800-53. *Security and Privacy Controls for Information Systems and Organizations.* 5. revize. U.S. Department of Commerce: National Institute of Standards and Technology, 2017.

[9] *Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).* [online]. [cit. 2019-02-18]. Dostupné z: https://www.govcert.cz/download/kii-vis/ZKB_uplne_zneni.pdf

[10] Zákon o kybernetické bezpečnosti: Přehledové blokové schéma k zákonu a jeho prováděcím předpisům. In: *NÚKIB: Národní úřad pro kybernetickou a informační bezpečnosti* [online]. Praha, 20. 2. 2018 [cit. 2019-04-01]. Dostupné z: https://www.govcert.cz/download/kii-vis/ZKB_blokove_schema.pdf

[11] Zákon o kybernetické bezpečnosti: Povinnosti orgánů a osob podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů. In: *NÚKIB: Národní úřad pro kybernetickou a informační bezpečnosti* [online]. Praha, 1. 8. 2017 [cit. 2019-04-01]. Dostupné z: https://www.govcert.cz/download/kii-vis/Schema_povinnosti.pdf

[12] *Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti).* [online]. [cit. 2019-02-18] Dostupné z: https://www.zakonyprolidi.cz/print/cs/2018-82/zneni-20180528.htm?sil=1

[13] Aktuální legislativa. In: *NCKB: Národní centrum kybernetické bezpečnosti* [online]. Praha [cit. 2019-05-01]. Dostupné z: https://www.govcert.cz/cs/regulace-a-kontrola/legislativa/

[14] Významné informační systémy: Proces určování podle vyhlášky č. 137/2014 Sb., o významných informačních systémech a jejich určujících kritériích. In: *NÚKIB: Národní úřad pro kybernetickou a informační bezpečnosti* [online]. Praha, 20. 3. 2018 [cit. 2019-04-01]. Dostupné z: https://www.govcert.cz/download/kii-vis/Schema_VIS.pdf

[15] Kritická informační infrastruktura: Proces určování podle zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon) a o nařízení vlády č.432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury ve znění novely č. 315/2014 Sb. In: *NÚKIB: Národní úřad pro kybernetickou a informační bezpečnosti* [online]. Praha, 20. 3. 2018 [cit. 2019-04-01]. Dostupné z: https://www.govcert.cz/download/kii-vis/Schema_KII.pdf

[16] Úřad pro ochranu osobních údajů. *Základní příručka k GDPR: Závazná podniková pravidla* [online]. 2013. Úřad pro ochranu osobních údajů. [cit. 2019-04-02]. Dostupné z: https://www.uoou.cz/zakladni-prirucka-k-gdpr/ds-4744/archiv=1&p1=3506

[17] ČSN ISO/IEC 27001 (36 9797) *Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Požadavky.* Praha: Český normalizační institut, 2014.

[18] ČSN ISO/IEC 27002, *Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Soubor postupů.* Praha: Český normalizační institut, 2014.

[19] DOUCEK, Petr. *Řízení bezpečnosti informací: 2. rozšířené vydání o BCM.* 2., přeprac. vyd. Praha: Professional Publishing, 2011. ISBN 978-80-7431-050-8.

[20] KONEČNÝ, Martin. *Pomůcka k auditu bezpečnostních opatření podle zákona o kybernetické bezpečnosti.* In: NCKB: Národní centrum kybernetické bezpečnosti [online]. Praha, 2015, 1. 5. 2015 [cit. 2019-05-01]. Dostupné z: https://www.govcert.cz/download/kii-vis/container-nodeid-580/vkbchecklistfinalv21rev.pdf

[21] KROUPOVÁ, Hana. *Metodika asistovaného zhodnocení*. Brno, 2019. Dostupné také z: https://www.vutbr.cz/studenti/zav-prace/detail/119719. Diplomová práce. Vysoké učení technické v Brně, Fakulta podnikatelská, Ústav informatiky. Vedoucí práce Petr Sedlák.

[22] Smlouvy. *Registr smluv* [online]. Praha: Ministerstvo vnitra ČR, 2016 [cit. 2019-05-04]. Dostupné z: https://smlouvy.gov.cz/

SEZNAM ZKRATEK

BCM	Business Continuity Management
CERT	Computer Emergency Response Team
CIA	confidentiality, integrity, availability
GDPR	General Data Protection Regulation
ICS	Industrial Control Systems
ICT	information and communication technology
IS	informační systém
ISMS	Information security management system
IT	Information Technology
KII	kritická informační infrastruktura
KS	komunikační systém
NIS	Network Information Security
NÚKIB	Národní úřad kybernetické a informační bezpečnosti
OÚ	osobní údaje
PDCA	plan, do, check, act
SIEM	Security Information and Event Management
VIS	významný informační systém
VKB	vyhláška o kybernetické bezpečnosti
ZKB	zákon o kybernetické bezpečnosti

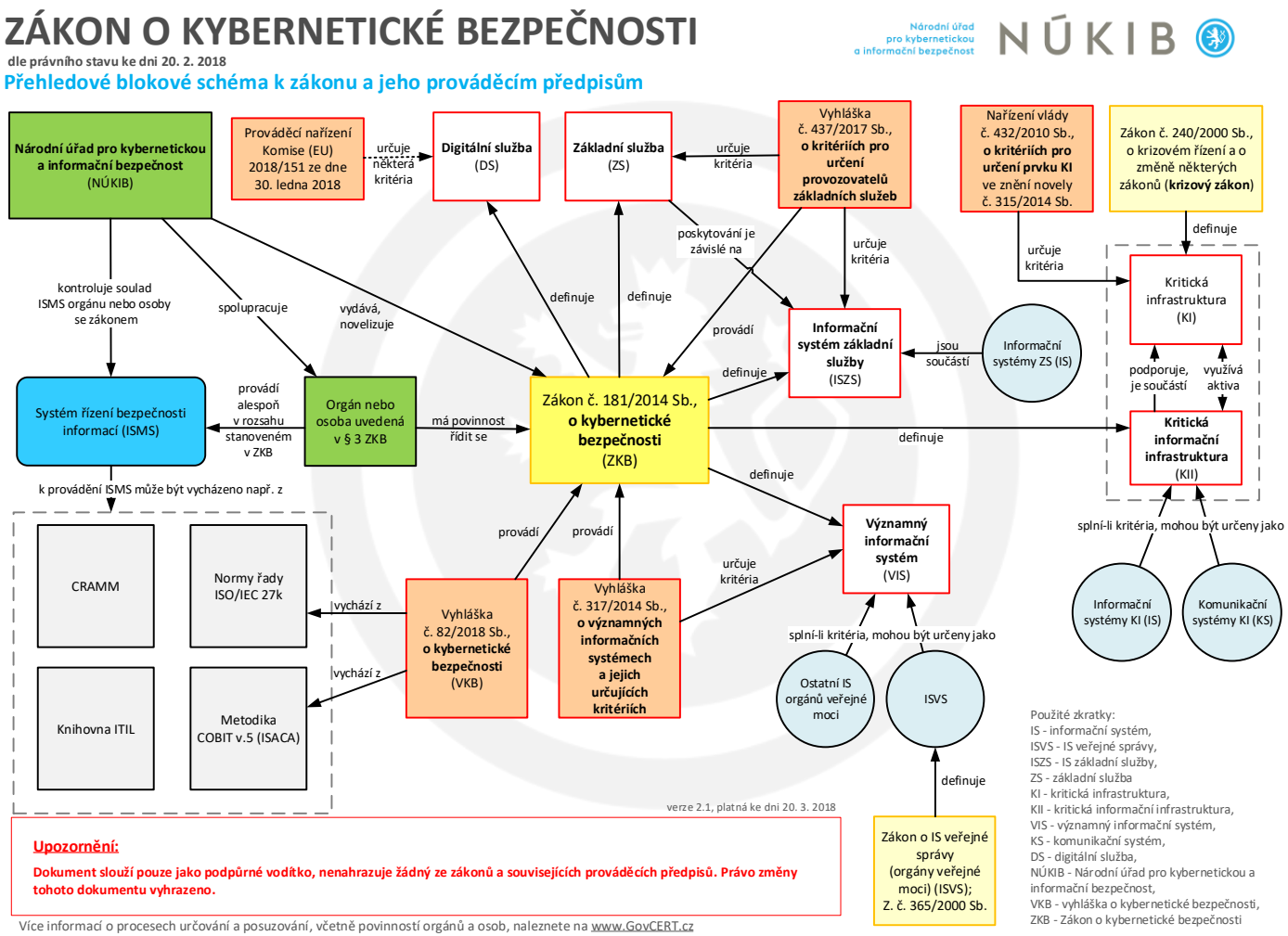
SEZNAM GRAFŮ

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

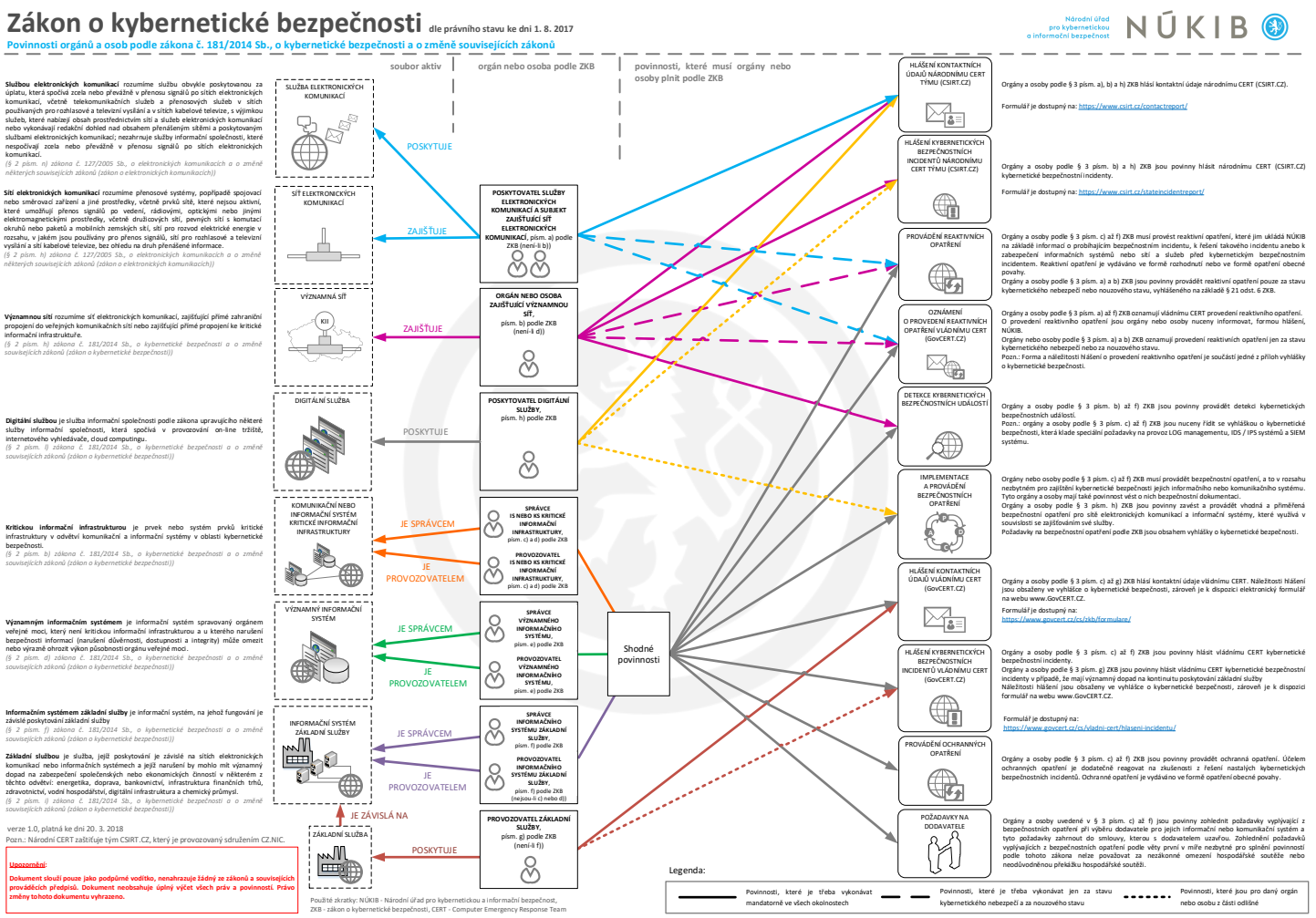
SEZNAM PŘÍLOH

Příloha 1: Přehledové blokové schéma k zákonu o kybernetické bezpečnosti a jeho prováděcím předpisům [10]



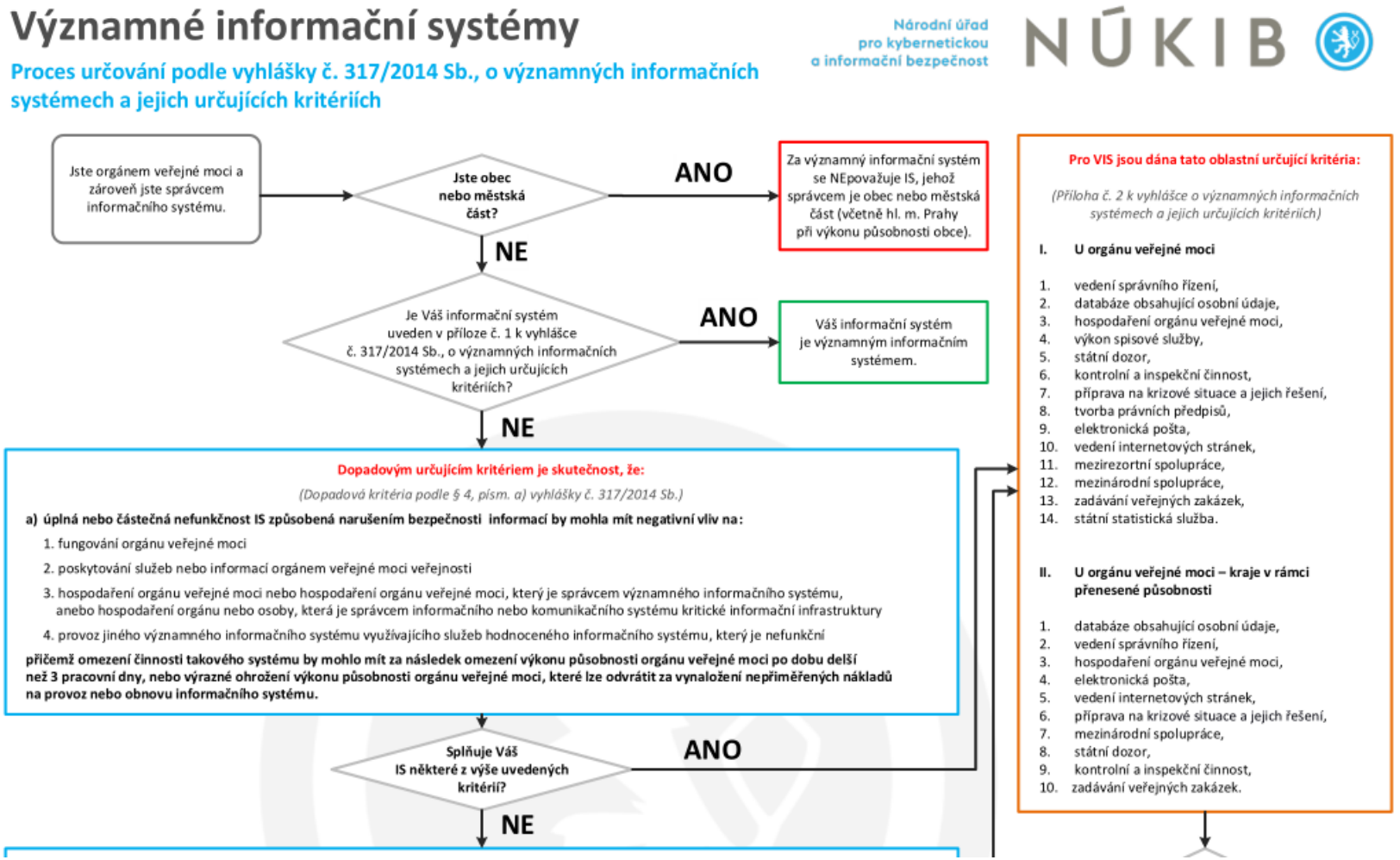
1.

Příloha 2: Povinnosti orgánů a osob podle kybernetického zákona [11]

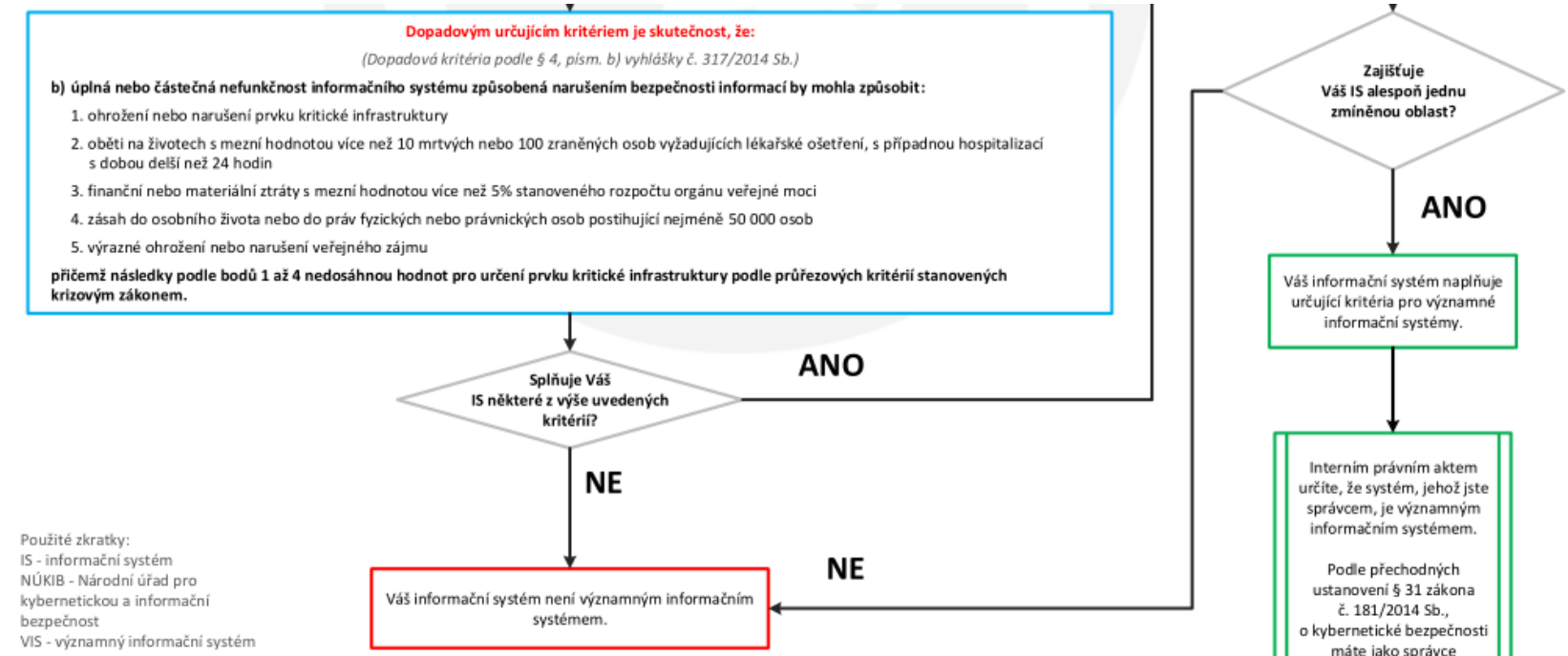


II:

Příloha 3: Proces určování významných informačních systémů [14]



III



Použité zkratky:
IS - informační systém
NÚKIB - Národní úřad pro kybernetickou a informační bezpečnost
VIS - významný informační systém

verze 2.0, platná ke dni 20. 3. 2018

Poznámka:

V rámci procesu určování významných informačních systémů je NÚKIB k dispozici k případnému jednání a k poskytnutí metodické pomoci v rámci posouzení naplnění určujících kritérií.

Naplnění určujících kritérií významného informačního systému, který není uveden v příloze č. 1 k vyhlášce o VIS, posuzuje správce informačního systému (viz. vyhláška č. 317/2014 Sb., § 3, odst. 3).

Upozornění:

Dokument slouží pouze jako podpůrné vodítko, nenahrazuje žádný ze zákonů a souvisejících prováděcích předpisů. Právo změny tohoto dokumentu vyhrazeno.

Více informací o procesech určování a posuzování, včetně povinností orgánů a osob, naleznete na www.GovCERT.cz

Příloha 4: Proces určování kritické informační infrastruktury [15]